Plec de prescripcions tècniques particulars que regeix la contractació relativa als Serveis de suport als Sistemes d'Informació, Infraestructures, Eines de Seguretat i Suport al Lloc de Treball de l'Agència

Exp. CO.04.2025

Índex

1 Introducció

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

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

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

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

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

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

Les xifres fan paleses la necessitat de dotar-se d'un Servei TIC que proporcioni el suport tecnològic necessari per a l'operativa de l'Agència de Ciberseguretat de Catalunya, assegurant la disponibilitat, la seguretat i l'eficiència dels seus sistemes d'informació. La gestió de més de 2.200 sistemes, amb més de 220.000 usuaris i un volum creixent d'amenaces, requereix una infraestructura TIC robusta i adaptada als alts estàndards de seguretat i resiliència.

Aquest servei intern és essencial per donar suport a les funcions de l'Agència, facilitant la gestió i protecció dels recursos tecnològics que permeten la seva operativa diària. Així, el Servei TIC de l'Agència s'encarrega d'assegurar el correcte funcionament de les plataformes, sistemes i eines tecnològiques, assegurant-ne la continuïtat i responent als requisits de seguretat i disponibilitat exigits en un entorn crític com és la ciberseguretat.

A més, aquest servei es troba alineat amb l'estratègia 2023-2027, "Una Catalunya Cibersegura en una Europa Digital", contribuint a l'eficiència operativa de l'Agència i reforçant la seva capacitat de resposta davant els reptes tecnològics actuals i futurs. Amb una gestió proactiva i orientada a la

millora contínua, el Servei TIC de l'Agència esdevé una peça clau per donar suport a la seva missió de protecció del ciberespai català.

1.1 Funcions de l'Agència rellevants a efectes de la nova estratègia de contractació

Avui en dia l'Agència té les següents funcions:

- **Gerència** s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació i la gestió de personal.
- **Operacions** du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció i resposta de seguretat en la seva vessant més operativa (coneguda com SOC/CERT).
- **Desenvolupament d'Estratègia d'Àmbits (DEA)** té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- **Producte i Centres de Competència i Innovació (DIP)** s'ocupa, per una banda, d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat. Per una altra banda, coordina, cohesiona i capacita l'ecosistema de la Ciberseguretat de Catalunya, recolzant el coneixement, sensibilització i conscienciació com a palanca de la transformació i creixement del sector.
- **Certificacions** desplega, en matèria de Ciberseguretat, 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

2.1 Context dels serveis objecte de la licitació

El servei objecte de la present licitació és el suport als Sistemes d'Informació, Infraestructures, Eines de Seguretat i Suport al Lloc de Treball de l'Agència (en endavant, Servei TIC). El Servei TIC es focalitza en la prestació d'un servei de suport especialitzat a l'Àrea de Tecnologia i Organització de l'Agència, que inclou tasques d'administració, operació i manteniment de les infraestructures, sistemes, solucions i eines, i s'articula en els àmbits funcionals següents:

- **Servei de Gestió i Operació de Plataformes i Infraestructura**: àmbit funcional de suport especialitzat a l'administració, operació, manteniment i evolució de les infraestructures, sistemes, xarxes, plataformes cloud i serveis associats de l'Agència, contribuint a la seva disponibilitat, seguretat, rendiment i continuïtat operativa.
- **Servei de Gestió i Suport de l'Espai de Treball Digital i Mobilitat**: àmbit funcional de suport a la gestió, operació i evolució de l'entorn digital de treball de l'Agència, incloent els dispositius corporatius, Microsoft 365, la identitat 365, la mobilitat, els espais de treball virtuals, l'accés remot segur i les eines de productivitat, amb l'objectiu de garantir una experiència d'usuari segura, eficient, governada i alineada amb les polítiques corporatives.
- **Servei de Gestió i Operació de la Seguretat i Compliment TIC**: àmbit funcional suport especialitzat a l'operació de les eines i controls de seguretat TIC de l'Agència, incloent la protecció d'identitats, accessos, dispositius, xarxes, serveis cloud i plataformes corporatives, així com la generació d'evidències, el seguiment de desviacions i el suport a les activitats de compliment normatiu, contribuint a mantenir un entorn tecnològic segur, traçable i alineat amb l'ENS, el marc normatiu aplicable i les polítiques internes de l'Agència, així com els estàndards de seguretat i les bones pràctiques per a la gestió de serveis TIC.
- **Servei de Gestió de la Transformació i Evolució Tecnològica i de la Seguretat**: àmbit funcional de suport especialitzat a la millora contínua, modernització i evolució del Servei TIC, mitjançant la identificació i execució d'actuacions d'automatització, integració, observabilitat, innovació, adopció de noves capacitats tecnològiques, intel·ligència artificial, optimització de processos i evolució de plataformes, contribuint a incrementar l'eficiència operativa, la qualitat del servei, la seguretat i l'alineament tecnològic amb les necessitats presents i futures de l'Agència.

El Servei TIC té un àmbit d'actuació transversal que implica donar suport a la integració operativa i executar la gestió tècnica de tots els àmbits funcionals sota les directrius, criteris i decisions de l'Agència, usant metodologies madures i reconegudes per la indústria, aportant i contribuint a la disponibilitat de les solucions tecnològiques que donen resposta a les necessitats de l'Agència, contribuint a la protecció de la informació, a la seguretat de les infraestructures i al suport eficient al lloc de treball, d'acord amb el model de seguretat i governança establert per l'Agència.

La prestació objecte del contracte té caràcter de suport tècnic especialitzat als serveis TIC de l'Agència, sota la direcció i governança del Servei TIC.

L'execució del contracte no implica la delegació ni externalització de les funcions de direcció, governança, planificació, priorització, control, arquitectura corporativa, supervisió, validació ni presa de decisions pròpies de l'Agència.

Correspon exclusivament a l'Agència:

- La definició de l'estratègia TIC
- El govern tecnològic
- La priorització de la demanda

- L'aprovació dels canvis rellevants
- La validació de les decisions tècniques
- La gestió pressupostària
- La governança de proveïdors
- L'exercici de les funcions públiques associades al servei

L'adjudicatari actuarà sempre sota les directrius, criteris i decisions adoptades per l'Agència.

2.2 Servei TIC

2.2.1 Objecte i abast del servei

El Servei TIC depèn orgànicament de l'Àrea de Tecnologia i Organització de l'Agència, però està orientat a proporcionar suport global a tota l'entitat. La seva missió principal és contribuir al correcte funcionament dels sistemes i infraestructures tecnològiques, oferir un suport integral que inclou la gestió i operació de les plataformes corporatives, les eines de seguretat i compliment TIC, la transformació i evolució contínua dels serveis i tecnologies de l'Agència, així com l'assistència tècnica a l'entorn de lloc de treball digital. Així, el Servei TIC assegura la disponibilitat, fiabilitat i protecció dels actius digitals de l'Agència, facilitant el desenvolupament eficient de les seves funcions estratègiques en matèria de ciberseguretat.

Les referències estratègiques, tecnològiques o d'evolució incloses en aquest apartat tenen per finalitat contextualitzar l'abast funcional del Servei TIC i orientar-ne l'execució. Les obligacions contractuals exigibles a l'adjudicatari són les activitats, funcionalitats, productes, lliurables, KPIs, ANS i evidències definides expressament en aquest plec, sempre dins del marc de governança, validació i decisió de l'Agència.

Donada la naturalesa de l'Agència com a entitat referent en ciberseguretat, la prestació objecte del contracte haurà d'ajustar-se als procediments establerts tant dins de l'organització com en la seva relació amb entitats externes, com el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) i altres administracions públiques. En aquest sentit, el Servei TIC ha de seguir les directrius i normes establertes per Seguretat Corporativa, adequar-se als requisits de l'Esquema Nacional de Seguretat (ENS) nivell alt i aplicar les bones pràctiques definides per l'ENS i la norma ISO/IEC 20000, com a referència de bones pràctiques per a la gestió de serveis TIC.

L'adjudicatari haurà d'assegurar el compliment d'aquests estàndards en tots els processos i àmbits del servei, proposant millores contínues en l'organització, administració i operació de les seves funcions. Així mateix, serà necessari establir una col·laboració estreta amb totes les àrees de l'Agència, especialment amb Seguretat Corporativa, per assegurar el compliment de l'ENS, i amb Aprovisionament, per gestionar de manera centralitzada la compra de maquinari, programari, subscripcions, suports i llicències.

El servei haurà d'incorporar tecnologies avançades com la intel·ligència artificial, l'automatització, l'observabilitat, la computació en el núvol, la ciberseguretat, la gestió de dades, les eines DevOps i la monitorització i gestió de recursos per contribuir a l'eficiència i seguretat del Servei TIC, detectar i prevenir amenaces de seguretat, automatitzar i optimitzar processos repetitius, reduir errors humans i millorar la productivitat. Així mateix, el servei haurà de contribuir a la preparació de la transició postquàntica dels sistemes i serveis sota el seu àmbit d'actuació, mitjançant la identificació de dependències criptogràfiques, l'anàlisi de riscos associats i la definició i manteniment actualitzat d'un full de ruta per a una transició ordenada cap a mecanismes criptogràfics resistents a la computació quàntica.

En particular, el Servei TIC haurà d'incorporar l'ús governat de capacitats d'intel·ligència artificial dins l'ecosistema Microsoft enterprise de l'Agència, especialment Microsoft 365 Copilot, Copilot Studio,

Security Copilot i altres capacitats d'IA o assistents intel·ligents que l'Agència determini, sempre que l'Agència disposi de les llicències, serveis, autoritzacions i condicions tècniques necessàries per al seu ús. Aquest ús haurà d'estar orientat a millorar l'eficiència operativa, la qualitat documental, la gestió del coneixement, l'automatització, l'anàlisi d'informació, la resposta a incidències, el suport al lloc de treball, la seguretat i el suport a la presa de decisions, sempre sota criteris de governança, seguretat, privacitat, traçabilitat, supervisió humana i compliment normatiu.

El Servei TIC haurà d'incorporar als seus procediments, la col·laboració i coordinació amb àmbits com la gestió d'incidents de seguretat, el suport en projectes de transformació de les diferents àrees de l'Agència i la gestió de canvis en sistemes no directament administrats pel servei. Aquesta coordinació es durà a terme tant internament com amb les entitats externes amb les quals col·labora l'Agència, contribuint a un servei eficient, segur i alineat amb els estàndards establerts.

Totes aquestes tasques de gestió, administració, operació i suport es duran a terme mitjançant l'execució coordinada dels àmbits funcionals descrits anteriorment. Aquesta coordinació haurà de proporcionar una visió integral de l'ecosistema tecnològic de l'Agència, afavorint l'observabilitat dels serveis, la correlació d'informació entre plataformes, la detecció anticipada de riscos i incidències, la millora contínua i el suport a la presa de decisions operatives i tecnològiques.

Els apartats següents diferencien entre els objectius estratègics del Servei TIC, les activitats i funcionalitats que haurà d'executar el servei, els productes i evidències que s'hauran de generar durant la prestació. Aquesta separació té per finalitat evitar solapaments, facilitar la traçabilitat contractual i assegurar una correspondència clara entre objectius, execució, lliurables i avaluació de les ofertes.

A efectes de coherència contractual, el Servei TIC inclou l'operació recurrent, l'administració, el suport, el manteniment, la documentació, la millora contínua i l'evolució ordinària dels àmbits funcionals descrits. No obstant això, les migracions massives, desplegaments extraordinaris, implantacions de noves plataformes no previstes, substitucions tecnològiques d'abast significatiu o projectes singulars que excedeixin la capacitat ordinària del servei requeriran planificació específica, aprovació prèvia de l'Agència i, si escau, el tractament contractual que correspongui.

2.2.2 Objectius del Servei

De manera transversal a tots els àmbits funcionals, el Servei TIC haurà de donar resposta als següents objectius estratègics:

- **Optimització i Expansió del Cloud**
- **Automatització i Integració Avançada**
- **Expansió i Optimització del Teletreball Segur**
- **Monitorització i Gestió automatitzada basada en IA**
- **Ciberseguretat com a servei (CSaaS)**
- **Transició Postquàntica i Criptoagilitat**
- **Adopció governada de la intel·ligència artificial i Copilot**
- **Estratègia de Continuïtat de Negoci Avançada**
- **Compliment i Governança al Cloud**
- **Innovació i Desenvolupament Continu**
- **Suport tècnic a la gestió de proveïdors de subministrament, material i llicències**

2.2.3 Activitats i funcionalitats

Les activitats i funcionalitats del Servei TIC hauran d'executar-se de manera alineada amb els objectius estratègics definits a l'apartat anterior, contribuint que l'operació diària, l'administració de plataformes, el suport al lloc de treball, la seguretat, l'automatització, la monitorització, la continuïtat i la governança tecnològica contribueixin de forma directa a la disponibilitat, seguretat, eficiència i evolució del servei.

Aquestes activitats s'hauran de desplegar sobre l'ecosistema tecnològic existent i previst de l'Agència, incloent, entre d'altres, Microsoft, Palo Alto, CrowdStrike, Cisco, Cohesity, Lansweeper, Nutanix, HPE, VMware, OTRS, Zabbix i ATOM/Remedy, així com qualsevol altra plataforma o eina que l'Agència determini durant la vigència del contracte. Nutanix s'haurà de considerar com a plataforma hiperconvergent prevista o potencialment destinada a substituir progressivament determinats components de l'entorn actual, d'acord amb les decisions tecnològiques que adopti l'Agència.

En aquest sentit, el servei haurà d'executar, com a mínim, les activitats i funcionalitats següents:

- **Activitats vinculades a l'optimització i expansió del cloud**: administrar, operar, optimitzar i donar suport a l'evolució dels entorns cloud de l'Agència, especialment sobre Azure i Microsoft 365, contribuint a una gestió segura, escalable i governada dels recursos. Aquestes activitats inclouran el suport a la migració progressiva de càrregues quan sigui viable, l'optimització de capacitat i consum, la revisió de configuracions, la gestió d'identitats i accessos, la integració amb serveis corporatius i la contribució a la reducció ordenada de dependències d'infraestructura pròpia, assegurant en tot moment que qualsevol acció es realitzi de forma controlada, traçable, alineada amb els estàndards corporatius i sostenibles des dels punts de vista temporal, tècnic i econòmic. **Activitats vinculades a l'automatització i integració avançada**: identificar, dissenyar, implantar, mantenir i documentar automatitzacions i integracions entre les eines corporatives del Servei TIC, les plataformes tecnològiques, els sistemes d'informació, els entorns cloud, els serveis de seguretat, l'inventari, la monitorització i la gestió de la demanda. Aquestes activitats hauran d'orientar-se a reduir intervencions manuals, minimitzar errors humans, millorar la qualitat i coherència de la dada, incrementar la traçabilitat, facilitar l'autoprovisionament governat, evitar sitges tecnològiques i proporcionar informació operativa i tècnica reutilitzable per al suport a la presa de decisions de l'Agència i la millora de l'eficiència del Servei TIC.
- **Activitats vinculades a l'expansió i optimització del teletreball segur**: donar suport operar el model de lloc de treball digital, mobilitat i accés remot segur desplegat actualment a l'Agència, incloent la gestió de dispositius, la gestió de polítiques de seguretat del lloc de treball i el suport a Microsoft 365 mitjançant Microsoft Intune, així com la gestió de llicenciament i el suport als models d'accés segur a recursos interns mitjançant Azure Virtual Desktop, Prisma Browser o les solucions equivalents que determini l'Agència. Aquestes activitats hauran de contribuir a una experiència d'usuari segura, governada, traçable i alineada amb les polítiques corporatives.
- **Activitats vinculades a la monitorització i gestió automatitzada basada en IA**: monitoritzar de manera contínua l'estat dels sistemes, serveis, xarxes, plataformes cloud, entorns de virtualització, còpies de seguretat, lloc de treball digital i components crítics mitjançant la solució existent, Zabbix, i les capacitats natives de les plataformes gestionades. El servei haurà d'analitzar alertes, detectar patrons, anticipar riscos, proposar accions preventives i, quan sigui viable i autoritzat per l'Agència, incorporar capacitats d'analítica avançada o intel·ligència artificial per millorar la detecció, la correlació d'esdeveniments, la classificació segons criteris de l'Agència i la resposta operativa.
- **Activitats vinculades a l'adopció governada de la intel·ligència artificial i Copilot:** identificar, proposar, dissenyar, preparar per a la validació i priorització de l'Agència i, un cop aprovats, operar els casos d'ús basats en Microsoft 365 Copilot, Copilot Studio, Security

Copilot i altres capacitats d'intel·ligència artificial autoritzades per l'Agència. Aquestes activitats hauran d'incloure, com a mínim, casos d'ús per a suport a usuaris, generació i revisió de documentació tècnica, consulta assistida de la base de coneixement, resum d'incidències i reunions, assistència en processos ITSM, automatització de respostes o fluxos amb Copilot Studio, anàlisi de senyals i incidents de seguretat amb Security Copilot, suport a la investigació tècnica, generació d'informes i identificació de millores operatives. Tots els casos d'ús hauran d'estar governats, documentats, validats per l'Agència i subjectes a criteris de seguretat, privacitat, qualitat de dades, supervisió humana, absència de decisions automàtiques no autoritzades i mesura de benefici.
Als efectes d'aquest contracte, s'entendrà per cas d'ús d'IA o Copilot qualsevol aplicació concreta, identificada, documentada i orientada a un objectiu de negoci o operatiu, que utilitzi capacitats d'intel·ligència artificial autoritzades per l'Agència per donar suport a processos, activitats, tasques o decisions associades al Servei TIC.

Cada cas d'ús haurà de disposar, com a mínim, de:

- Identificador únic.
- Nom i descripció.
- Objectiu i benefici esperat.
- Procés o activitat sobre el qual actua.
- Capacitat d'intel·ligència artificial utilitzada.
- Dades o fonts d'informació utilitzades.
- Responsable funcional.
- Controls de seguretat i privacitat aplicables.
- Mecanismes de supervisió humana.
- Indicadors de mesura del benefici.
- Estat (identificat, en validació, pilot, producció o retirat).

No es consideraran casos d'ús les proves puntuals, consultes aïllades, demostracions, activitats exploratòries sense objectiu definit ni l'ús genèric d'eines d'intel·ligència artificial sense governança associada.

- **Activitats vinculades a la ciberseguretat com a servei (CSaaS)**: operar, mantenir i coordinar les eines de seguretat vinculades als sistemes, lloc de treball, xarxa i accés remot ja mencionades i altres capacitats que determini l'Agència. Aquestes activitats hauran d'assegurar l'aplicació de polítiques, la revisió de configuracions, la traçabilitat d'accessos, el suport a la gestió d'incidents, la coordinació amb Seguretat Corporativa i la contribució al compliment dels requisits normatius, interns i contractuals aplicables, sense substituir les funcions pròpies dels serveis SOC, CERT o equivalents quan aquests estiguin definits fora de l'abast del Servei TIC.
- **Activitats vinculades a la transició postquàntica i criptoagilitat:** preparar l'evolució progressiva dels sistemes, serveis i plataformes de l'Agència cap a mecanismes criptogràfics resistents a la computació quàntica, mitjançant la identificació de dependències criptogràfiques, l'avaluació dels riscos associats, la definició i manteniment d'un full de ruta de transició postquàntica, l'impuls de criteris de criptoagilitat i el seguiment de les directrius i estàndards que esdevinguin aplicables.
- **Activitats vinculades a l'estratègia de continuïtat de negoci avançada**: operar i mantenir els mecanismes de disponibilitat, còpia de seguretat, recuperació i continuïtat associats a les plataformes gestionades, amb especial atenció a Cohesity, entorns de virtualització, infraestructures crítiques, serveis cloud i components de xarxa. El servei haurà de donar suport a la preparació, execució i documentació dels procediments de recuperació, proves de restauració, plans de contingència, anàlisi de riscos operatius i accions de millora, sempre sota validació de l'Agència.
- **Activitats vinculades al compliment i governança al cloud**: aplicar criteris de governança, seguretat, control de costos, etiquetatge, traçabilitat, gestió d'identitats, segregació de funcions i compliment normatiu en els serveis cloud gestionats. El servei haurà de preparar per a la validació de l'Agència les polítiques de govern cloud, executar, revisar configuracions,

aportar evidències de compliment i facilitar informació útil per al control tècnic, econòmic i operatiu dels entorns cloud.

- **Activitats vinculades a la innovació i desenvolupament continu**: identificar oportunitats de millora, racionalització, modernització i evolució tecnològica dels serveis, prioritzant solucions documentades, suportades pel fabricant, compatibles amb els estàndards corporatius i sostenibles operativament durant la vigència del contracte. El servei haurà de proposar millores basades en dades, analitzar-ne el benefici esperat, estimar-ne l'impacte tècnic, econòmic i organitzatiu, executar-les quan siguin aprovades per l'Agència i documentar-ne els resultats i evidències associades. A aquests efectes, l'adjudicatari haurà d'incorporar en l'informe mensual o trimestral de seguiment, segons determini l'Agència, un apartat específic de millora contínua que inclogui les propostes identificades, la seva justificació, benefici esperat, impacte tècnic, econòmic i organitzatiu, riscos associats, dependències, esforç estimat, priorització proposada, estat d'aprovació, execució i evidències de resultat quan correspongui.
- **Activitats vinculades al suport tècnic a la gestió de proveïdors de subministrament, material i llicències**: donar suport tècnic i operatiu als processos d'aprovisionament de maquinari, programari, subscripcions, suports i llicències, en coordinació amb l'Agència i les àrees responsables. Aquest suport inclourà la identificació de necessitats, validació tècnica, control d'inventari, seguiment de renovacions, optimització d'ús, traçabilitat de llicenciament, suport a la planificació pressupostària i contribució a la reducció de riscos de sobrecost, infrautilització o dependència tecnològica.

A més de les activitats i funcionalitats pròpies dels diferents àmbits funcionals, l'adjudicatari haurà de desenvolupar de forma transversal les activitats necessàries per garantir la correcta prestació, coordinació, governança i millora contínua del Servei TIC.

Com a mínim, aquestes funcions inclouran:

- Mantenir actualitzada la documentació tècnica, operativa i de gestió del servei en els repositoris corporatius establerts per l'Agència.
- Participar en els mecanismes de coordinació i relació amb les àrees internes de l'Agència, el CTTI, altres proveïdors i tercers involucrats en la prestació del servei.
- Participar en reunions de seguiment, gestionar escalats operatius i contribuir a la resolució de conflictes o dependències que puguin afectar el servei.
- Contribuir a la implantació de mesures d'automatització, industrialització i millora contínua dels processos i serveis.
- Mantenir alineada la prestació del servei amb els objectius estratègics, operatius i tecnològics definits per l'Agència.
- Contribuir al seguiment de la capacitat, riscos, dependències i estat general dels serveis gestionats.
- Generar, mantenir i actualitzar els indicadors, informes, quadres de comandament i evidències necessàries per al seguiment del servei.
- Identificar, analitzar i proposar millores tècniques, operatives, organitzatives o metodològiques orientades a incrementar l'eficiència, la seguretat, la qualitat i la sostenibilitat del servei.
- Analitzar noves tecnologies, eines i capacitats que puguin aportar millores al servei i formular les corresponents propostes per a la seva valoració per part de l'Agència.
- Contribuir a millorar la visibilitat, comprensió i comunicació dels resultats, activitats i beneficis generats pel servei mitjançant informes, mètriques, quadres de comandament i altres mecanismes de reporting..

2.2.4 Productes, lliurables i KPIs del Servei TIC

Als efectes d'aquest apartat, s'entén per producte qualsevol solució, plataforma, entorn, repositori, catàleg, model o pla que constitueixi un resultat governable, mesurable, reutilitzable i verificable del

Servei TIC. Els productes següents no substitueixen les activitats operatives descrites a l'apartat anterior, sinó que n'agrupen les evidències, capacitats i resultats esperats per facilitar el govern contractual, la traçabilitat, la continuïtat operativa i l'avaluació del compliment.

Els KPIs inclosos en aquest apartat tenen naturalesa d'indicadors de seguiment, governança, control i millora contínua del Servei TIC. Només tindran caràcter penalitzable quan estiguin expressament recollits com a ANS al capítol 4 o quan el contracte així ho estableixi. Els ANS, per tant, constitueixen els compromisos contractuals exigibles i subjectes al règim de penalitzacions corresponent, mentre que els KPIs serveixen per mesurar l'evolució, qualitat i maduresa del servei.

- **Solució d'observabilitat, monitorització i AIOps:** Producte orientat a disposar d'una capacitat transversal de visibilitat, supervisió, correlació i anàlisi del comportament dels sistemes, serveis, xarxes, entorns cloud, lloc de treball, backup, seguretat i components crítics del Servei TIC.

Element	Descripció
Finalitat	Disposar d'una capacitat transversal de visibilitat, supervisió, correlació i anàlisi del comportament dels sistemes, serveis, xarxes, entorns cloud, lloc de treball, backup i seguretat.
Plataformes principals	Zabbix, Azure Monitor, Log Analytics, Application Insights, Microsoft Defender, Microsoft 365.
Lliurables mínims	Informe de disponibilitat, quadres de comandament, registre d'alertes, procediments de monitorització, evidències de revisió de llindars, informes de capacitat i full de ruta AIOps.
KPIs	% incidències detectades proactivament; % reducció soroll d'alertes; % disponibilitat monitorització; % alertes crítiques amb diagnòstic documentat.
Evidències	Informes mensuals, extraccions de Zabbix/Azure Monitor, quadres de comandament, actes de revisió i registres de tiquets.
ANS relacionats	STICOBS01, STICDISP01, STICGOV01.

- **Plataforma ITSM i suport al govern de la demanda del Servei TIC:** Producte orientat a disposar d'una plataforma centralitzada per al registre, classificació, priorització, seguiment i suport al govern de la demanda del Servei TIC, incloent incidents, peticions, problemes, canvis, tasques, backlog i fluxos de treball associats.

Element	Descripció
Finalitat	Disposar d'una plataforma centralitzada per al registre, classificació, proposta de priorització, seguiment i suport al govern de la demanda del Servei TIC per part de l'Agència, incloent incidents, peticions, problemes, canvis, tasques, backlog i fluxos de treball associats.
Plataformes principals	OTRS i eines corporatives que determini l'Agència, amb integració amb monitorització, inventari, documentació, automatització i reporting.
Lliurables mínims	Informes d'incidents, peticions, problemes i canvis; informe de compliment d'ANS; registre de backlog i demanda; catàleg de serveis, categories i fluxos ITSM; evidències de tancament i validació; informes de recurrència i causes arrel; propostes de millora i automatització dels processos ITSM.
KPIs	% de tiquets resolts dins dels ANS establerts; temps mitjà de resolució d'incidents i peticions; nombre de tiquets en backlog obert i evolució mensual; % de tiquets amb categorització, prioritat i tancament validat.

Evidències	Extraccions d'OTRS, informes mensuals, quadres de comandament ITSM, registres de tiquets, actes de revisió, evidències de tancament, informes de recurrència i plans d'acció.
ANS relacionats	STICITSM01, STICITSM02, STICGOV01.

- **Solució d'identitat, accés i gestió de dispositius:** Producte orientat a disposar d'una capacitat integrada de suport al govern d'identitats, accessos, dispositius, perfils, permisos i polítiques de compliment del Servei TIC.

Element	Descripció
Finalitat	Disposar d'una capacitat integrada de suport al govern d'identitats, accessos, dispositius, perfils, permisos i polítiques de compliment del Servei TIC.
Plataformes principals	Entra ID, Intune, Microsoft 365 i capacitats associades que determini l'Agència.
Lliurables mínims	Inventari d'identitats, dispositius i perfils gestionats; evidències d'aplicació de polítiques; informes de compliment de dispositius; registres d'altes, baixes i modificacions; evidències de revisió d'accessos, rols i permisos privilegiats; procediments d'enrolament, baixa i canvi; informes de desviacions i riscos.
KPIs	% de dispositius conformes amb les polítiques corporatives; % d'identitats amb revisió d'accessos vigent; temps mitjà de tramitació d'altes, baixes i modificacions; % de dispositius inventariats i associats correctament a usuari o perfil.
Evidències	Informes d'Intune i Entra ID, registres d'altes, baixes i modificacions, evidències de polítiques aplicades, informes de compliment, registres de revisió d'accessos, inventari de dispositius i actes de validació.
ANS relacionats	STICIDM01, STICSEC01, STICGOV01.

- **Solució de protecció endpoint, xarxa i accés segur:** Producte orientat a disposar d'una capacitat integrada de protecció, control, visibilitat i traçabilitat sobre endpoints, xarxa corporativa, accés remot i navegació segura.

Element	Descripció
Finalitat	Disposar d'una capacitat integrada de protecció, control, visibilitat i traçabilitat sobre endpoints, xarxa corporativa, accés remot i navegació segura, coordinada amb el model corporatiu de seguretat i sense substituir les funcions pròpies dels serveis SOC, CERT o equivalents fora de l'abast del Servei TIC.
Plataformes principals	Microsoft Defender, CrowdStrike, Palo Alto, Prisma Access, Prisma Browser i capacitats equivalents que determini l'Agència.
Lliurables mínims	Evidències de configuració i aplicació de polítiques; informes d'estat de protecció endpoint; registres d'alertes i actuacions; evidències de revisió de permisos i accessos; informes de compliment ENS i polítiques internes; registre d'incidents de seguretat coordinats; plans d'acció i seguiment de remediacions.
KPIs	% d'endpoints protegits i reportant correctament; % d'accessos remots traçables i conformes a política; temps mitjà de remediació de desviacions de seguretat; % de polítiques crítiques revisades dins del període establert.
Evidències	Informes de Defender, CrowdStrike, Palo Alto, Prisma Access o Prisma Browser; registres d'alertes; evidències de configuració; registres de revisió d'accessos; informes de compliment; tiquets de remediació i actes de validació.

ANS relacionats	STICSEC01, STICIDM01, STICGOV01.

- **Model d'intel·ligència artificial, Copilot i casos d'ús governats:** Producte orientat a disposar d'un model d'adopció, governança, explotació i millora contínua de les capacitats d'intel·ligència artificial aplicables al Servei TIC, especialment Microsoft 365 Copilot, Copilot Studio i Security Copilot.

Element	Descripció
Finalitat	Disposar d'un model d'adopció, suport al govern de l'Agència, explotació i millora contínua de les capacitats d'intel·ligència artificial aplicables al Servei TIC, especialment Microsoft 365 Copilot, Copilot Studio i Security Copilot, executant les mesures de seguretat establertes per l'Agència, privacitat, compliment normatiu, traçabilitat, qualitat de dades, supervisió humana i integració amb el tenant Microsoft 365 de l'Agència.
Plataformes principals	Microsoft 365 Copilot, Copilot Studio, Security Copilot i altres capacitats d'intel·ligència artificial autoritzades per l'Agència.
Lliurables mínims	Mapa de casos d'ús d'IA i Copilot; criteris de proposta de priorització i valoració; fitxes de casos d'ús amb objectiu, àmbit, dades utilitzades, riscos, controls, benefici esperat i indicadors; guia d'ús segur de Copilot; registre d'evidències per a la validació de l'Agència; evidències de proves pilot; informes d'adopció i ús; procediments d'operació i suport al govern; registre de millores identificades; materials de formació i transferència de coneixement.
KPIs	Nombre de casos d'ús d'IA identificats, amb proposta de priorització i preparats per a la validació de l'Agència; % de casos d'ús amb controls de seguretat i privacitat documentats; reducció estimada de temps en processos suportats per IA; % de documentació o consultes resoltes amb suport de base de coneixement i Copilot; nombre d'automatitzacions o agents creats amb Copilot Studio i aprovats per l'Agència; nombre d'investigacions o anàlisis de seguretat assistides per Security Copilot; nivell d'adopció i satisfacció dels usuaris autoritzats.
Evidències	Fitxes de casos d'ús aprovades, registres de validació, informes d'adopció, evidències de proves pilot, registres d'ús, materials de formació, actes de revisió, quadres de comandament, informes de benefici i evidències de controls de seguretat, privacitat i supervisió humana.
ANS relacionats	STICIA01, STICAUT01, STICDOC01, STICGOV01.

- **Entorn cloud i Microsoft 365:** Producte orientat a disposar d'un entorn cloud i SaaS segur, escalable, governat i eficient, integrat pels serveis Azure, Microsoft 365 i la resta de plataformes corporatives que determini l'Agència.

Element	Contingut
Finalitat	Disposar d'un entorn cloud i SaaS segur, escalable, governat i eficient, integrat pels serveis Azure, Microsoft 365 i la resta de plataformes corporatives que determini l'Agència, amb control sobre configuració, identitat, seguretat, capacitat, consum, llicenciament, integració, etiquetatge, compliment i evolució tecnològica.
Plataformes principals	Azure, Microsoft 365, Entra ID, Intune, Defender, Azure Monitor, Log Analytics i altres serveis cloud o SaaS corporatius autoritzats per l'Agència.
Lliurables mínims	Informes d'ús, capacitat i consum; evidències de configuració segura; informes de llicenciament i assignació; registres de canvis i optimitzacions; quadres de

	comandament cloud; informes de riscos i desviacions; propostes d'optimització tècnica i econòmica.
KPIs	% de recursos cloud etiquetats i classificats correctament; desviació mensual de consum cloud respecte al pressupost o previsió; % de configuracions crítiques conformes a política; % de llicències assignades amb ús efectiu o justificat.
Evidències	Informes d'Azure, Microsoft 365 i Entra ID; quadres de comandament; registres de canvis; informes de consum i llicenciament; evidències de configuració; informes de riscos, desviacions i accions de remediació.
ANS relacionats	STICCLOUD01, STICIDM01, STICSEC01, STICGOV01.

- **Solució de backup, recuperació i continuïtat:** Producte orientat a disposar d'una capacitat documentada, verificable i alineada amb els requisits de disponibilitat, recuperació i continuïtat operativa dels actius i serveis gestionats.

Element	Contingut
Finalitat	Disposar d'una capacitat documentada, verificable i alineada amb els requisits de disponibilitat, recuperació i continuïtat operativa dels actius i serveis gestionats, assegurant cobertura de còpies, recuperabilitat, proves, control de riscos i alineació amb els requeriments de disponibilitat, seguretat i continuïtat de negoci de l'Agència.
Plataformes principals	Cohesity, Azure Backup i capacitats associades a les plataformes corporatives que determini l'Agència.
Lliurables mínims	Informes d'execució de còpies; evidències de restauració; registre d'errors i incidències de backup; procediments de recuperació; resultats de proves de restauració; informes de cobertura i capacitat; pla d'accions correctives.
KPIs	% de còpies executades correctament; % de restauracions provades amb resultat satisfactori; temps mitjà de recuperació en proves o incidents; % d'actius crítics coberts per política de backup.
Evidències	Informes de Cohesity o Azure Backup, registres d'execució, evidències de proves de restauració, informes d'errors, procediments validats, informes de cobertura, plans d'acció i actes de revisió.
ANS relacionats	STICBCK01, STICBCK02, STICCONT01, STICGOV01.

- **Repositori d'actius, CMDB i mapa de serveis TIC:** Producte orientat a disposar d'una font autoritativa, estructurada, actualitzada i explotable d'informació sobre actius TIC, elements de configuració, relacions, dependències, configuracions, ubicació, criticitat, titularitat i mapa de serveis.

Element	Contingut
Finalitat	Disposar d'una font autoritativa, estructurada, actualitzada i explotable d'informació sobre actius TIC, elements de configuració, relacions, dependències, configuracions, ubicació, criticitat, titularitat i mapa de serveis.
Plataformes principals	Lansweeper, CMDB i eines corporatives d'inventari, ITSM, monitorització, documentació i reporting que determini l'Agència.
Lliurables mínims	Inventari actualitzat d'actius i CIs; mapa de serveis i dependències; informes de qualitat de la dada; registre de canvis sobre actius; informes d'obsolescència i riscos; evidències de conciliació amb altres eines; quadres de comandament d'inventari.

KPIs	% d'actius inventariats amb dades completes; % de CIs amb relacions i dependències documentades; nombre de discrepàncies detectades en conciliacions; % de canvis vinculats a actius o CIs actualitzats.
Evidències	Extraccions de Lansweeper o CMDB, informes de conciliació, registres de canvis, informes de qualitat de la dada, mapa de dependències, quadres de comandament i actes de revisió.
ANS relacionats	STICCMDB01, STICGOV01, STICREP01.

- **Entorn de workplace digital i accés remot segur:** Producte orientat a disposar d'un entorn de treball digital segur, homogeni, governat i eficient per als usuaris interns i col·laboradors de l'Agència.

Element	Contingut
Finalitat	Disposar d'un entorn de treball digital segur, homogeni, governat i eficient per als usuaris interns i col·laboradors de l'Agència, garantint accés segur, gestió del parc de dispositius, mobilitat, teletreball segur i qualitat de l'experiència d'usuari.
Plataformes principals	Microsoft 365, Intune, Azure Virtual Desktop, Prisma Browser i solucions equivalents que determini l'Agència.
Lliurables mínims	Informes d'estat del parc de dispositius; registres d'incidències i peticions workplace; evidències de polítiques aplicades; procediments d'alta, baixa i suport; informes d'ús d'AVD o accés remot; evidències de compliment del lloc de treball; propostes de millora d'experiència d'usuari.
KPIs	% de dispositius workplace conformes; temps mitjà de resolució d'incidències workplace; % d'usuaris amb accés remot operatiu i conforme; nivell de satisfacció o qualitat percebuda del lloc de treball digital.
Evidències	Informes d'Intune, Microsoft 365, AVD o Prisma Browser, registres ITSM, evidències de polítiques, informes d'ús, registres de suport, enquestes o indicadors de qualitat percebuda i actes de revisió.
ANS relacionats	STICIDM01, STICITSM01, STICITSM02, STICSEC01.

- **Catàleg d'automatització, integració i orquestració:** Producte orientat a disposar d'un conjunt ordenat, documentat, versionat i governat d'automatitzacions, scripts, runbooks, fluxos, plantilles, integracions i mecanismes d'autoprovisionament del Servei TIC.

Element	Contingut
Finalitat	Disposar d'un conjunt ordenat, documentat, versionat i governat d'automatitzacions, scripts, runbooks, fluxos, plantilles, integracions i mecanismes d'autoprovisionament del Servei TIC, orientat a reduir intervencions manuals, millorar la qualitat de la dada, incrementar la traçabilitat i reforçar l'eficiència operativa.
Plataformes principals	Azure Automation, PowerShell, Power Automate, Copilot Studio, OTRS, Zabbix, Lansweeper, Intune, Azure, Microsoft 365, Cohesity i plataformes de seguretat autoritzades.
Lliurables mínims	Catàleg d'automatitzacions; scripts i runbooks documentats; fluxos i integracions validades; evidències de proves; registre de versions; procediments d'execució i manteniment; informe de benefici obtingut.

KPIs	Nombre d'automatitzacions actives i documentades; % d'operacions recurrents automatitzades; temps estalviat estimat per automatització; % d'automatitzacions amb proves i control de versions vigent.
Evidències	Repositori de scripts o runbooks, registre de versions, evidències de proves, registres d'execució, documentació tècnica, actes de validació, informes de benefici i quadres de seguiment.
ANS relacionats	STICAUT01, STICGOV01, STICREP01.

- **Model de governança, reporting i millora contínua:** Producte orientat a disposar d'un model transversal de suport al govern, seguiment, control i millora del Servei TIC per part de l'Agència, basat en indicadors, riscos, ANS, qualitat, capacitat, consum, dedicació, estat dels serveis, evolució tecnològica, millores i compromisos, incloent la definició, seguiment i actualització del pla de capacitat dels serveis i plataformes sota abast

Element	Contingut
Finalitat	Disposar d'un model transversal de govern, seguiment, control i millora del Servei TIC, basat en indicadors, riscos, ANS, qualitat, capacitat, consum, dedicació, estat dels serveis, evolució tecnològica, millores i compromisos.
Plataformes principals	OTRS, Zabbix, Lansweeper, Microsoft 365, SharePoint, Teams, Power BI o eines corporatives equivalents que determini l'Agència.
Lliurables mínims	Informe mensual de servei; informe executiu de seguiment; quadre de comandament transversal; registre de riscos; registre de millores; seguiment d'ANS; actes i acords de comitès; informe de consum, dedicació i capacitat.
KPIs	% d'ANS complerts; % d'informes lliurats dins del termini establert; nombre de riscos oberts i evolució mensual; % d'accions de millora completades dins del termini acordat.
Evidències	Informes mensuals, quadres de comandament, registres de riscos i millores, actes de comitè, extraccions d'eines corporatives, evidències de tancament d'accions i validacions de l'Agència.
ANS relacionats	STICGOV01, STICREP01, STICPER01.

- **Repositori documental i base de coneixement:** Producte orientat a disposar d'un repositori estructurat, actualitzat, accessible i reutilitzable del coneixement tècnic i operatiu, sota els criteris de govern documental establerts per l'Agència.

Element	Contingut
Finalitat	Disposar d'un repositori estructurat, actualitzat, accessible i reutilitzable del coneixement tècnic i operatiu del Servei TIC, sota els criteris de govern documental establerts per l'Agència, contribuint a la continuïtat, qualitat documental, propietat de l'Agència i transferència efectiva de coneixement.
Plataformes principals	SharePoint, OneDrive, Teams, Microsoft 365, formats Markdown i eines autoritzades de gestió del coneixement com Obsidian o equivalents.
Lliurables mínims	Repositori documental actualitzat; procediments operatius; manuals tècnics; guies de suport; base de coneixement; inventari de documentació; registre de revisions; pla de transferència de coneixement.
KPIs	% de documentació crítica actualitzada dins del període establert; % de procediments validats per l'Agència; nombre d'articles o guies reutilitzables

	incorporades a la base de coneixement; % de documents amb responsable, versió i data de revisió informada.
Evidències	Inventari documental, registres de versions i revisions, repositori corporatiu, actes de validació, evidències de transferència de coneixement, documents actualitzats i informes de qualitat documental.
ANS relacionats	STICDOC01, STICREP01, STICGOV01, STICREV01.

- **Pla de transició, evolució tecnològica i reversibilitat:** Producte orientat a disposar d'un instrument formal per ordenar la transició inicial, l'evolució tecnològica, les migracions, la substitució progressiva de plataformes, la gestió del canvi i la reversibilitat final del contracte.

Element	Contingut
Finalitat	Disposar d'un instrument formal per ordenar la transició inicial, l'evolució tecnològica, les migracions, la substitució progressiva de plataformes, la gestió del canvi i la reversibilitat final del contracte, minimitzant riscos, impacte operatiu i dependències del proveïdor.
Plataformes principals	Eines corporatives de gestió de projectes, ITSM, repositori documental, CMDB, inventari, monitorització, Microsoft 365 i plataformes tecnològiques afectades per la transició o evolució.
Lliurables mínims	Pla de transició inicial; pla d'evolució tecnològica; registre de canvis rellevants; documentació de migracions; evidències de validació; pla de reversibilitat; informe final de traspàs; acta de lliurament de coneixement.
KPIs	% de fites de transició completades dins del termini acordat; % de migracions o canvis rellevants amb evidències de validació; nombre d'incidències atribuïbles a transicions o canvis tecnològics; % de documentació de reversibilitat validada i actualitzada.
Evidències	Plans aprovats, registres de canvis, actes de validació, evidències de migració, documentació de reversibilitat, inventaris actualitzats, actes de traspàs i informes finals de transició.
ANS relacionats	STICREV01, STICCONT01, STICDOC01, STICGOV01.

2.2.5 Característiques del servei

Aquest apartat descriu les característiques essencials que hauran de regir la prestació del Servei TIC durant l'execució del contracte. Aquestes característiques concreten els requisits funcionals, operatius, tècnics, organitzatius, de governança, seguretat, documentació, seguiment i qualitat que haurà de complir el servei, sense introduir prestacions independents ni substituir els criteris de valoració establerts en la documentació administrativa corresponent.

Característiques exigibles del servei:

- **Model de suport i prestació del Servei TIC:** el servei haurà de disposar d'un model de suport i execució que cobreixi, com a mínim, els àmbits d'infraestructura, sistemes, cloud, Microsoft 365, lloc de treball digital, identitat, accés segur, xarxa, seguretat TIC, backup, monitorització, ITSM, inventari, documentació, automatització, governança i suport a l'evolució tecnològica. Aquest model haurà de garantir l'execució coordinada de les activitats recurrents, el suport a projectes, la gestió de canvis, la resolució d'incidències, la gestió de peticions, la millora contínua i la coordinació amb l'Agència, Seguretat Corporativa, Aprovisionament, CTTI, altres proveïdors i equips interns o externs relacionats amb el servei.

- **Adequació a l'ecosistema tecnològic de l'Agència:** El servei haurà d'operar, mantenir, integrar i evolucionar les plataformes i eines existents o previstes de l'Agència, incloent, entre d'altres, Azure, Microsoft 365, Entra ID, Intune, Defender, Azure Virtual Desktop, Copilot 365, Palo Alto, Prisma Access, Prisma Browser, CrowdStrike, Cisco, VMware, Nutanix, HPE, Cohesity, OTRS, Zabbix, Lansweeper, ATOM/Remedy i qualsevol altra eina corporativa que determini l'Agència durant la vigència del contracte. L'adequació a aquest ecosistema haurà de contribuir a la disponibilitat i continuïtat operativa, la seguretat, la interoperabilitat, la traçabilitat, la governança i l'eficiència en l'ús de les plataformes corporatives.
    - **Model d'equip, rols i dedicacions:** el servei haurà de disposar d'una organització operativa suficient per cobrir tots els àmbits funcionals del contracte, amb rols, responsabilitats, dedicacions, mecanismes de coordinació, substitució, retenció del coneixement, suport especialitzat i escalat adequats a la criticitat del servei. El dimensionament i l'organització del servei hauran d'assegurar la capacitat real per complir els ANS, assegurar la continuïtat operativa, evitar dependències individuals excessives i mantenir la cobertura funcional durant tota la vigència del contracte.
    - **Model de suport a la governança, seguiment i relació:** el servei haurà de disposar d'un model de suport a la governança, seguiment i relació que inclogui comitès, interlocutors, circuits d'escalat, mecanismes de suport a la presa de decisions, seguiment d'ANS, suport al seguiment econòmic-operatiu, aportació d'informació per al control de capacitat, gestió de riscos, classificació de la demanda segons criteris de l'Agència i coordinació amb l'Agència i la resta d'agents implicats. Aquest model haurà de proporcionar informació periòdica, fiable, traçable i orientada al suport a la presa de decisions de l'Agència, d'acord amb els formats, canals, periodicitats i òrgans de seguiment que determini l'Agència.
    - **Model ITSM i gestió de la demanda:** el servei haurà de disposar d'un model ITSM per gestionar incidents, peticions, problemes, canvis, tasques, backlog i fluxos de treball, incloent classificació, proposta de priorització segons criteris de l'Agència, escalat, qualitat del registre, aportació d'informació per al control dels ANS, anàlisi de recurrències i integració amb OTRS, monitorització, CMDB, documentació, reporting i automatitzacions. Aquest model haurà d'assegurar la traçabilitat d'extrem a extrem de la demanda, la qualitat de la informació registrada, la capacitat de seguiment i la disponibilitat d'evidències suficients per al govern del servei per part de l'Agència.
- **Seguretat, compliment i traçabilitat:** el servei haurà d'executar l'aplicació de les polítiques de seguretat de l'Agència, el compliment de l'ENS i del marc normatiu aplicable, el control d'accessos, la segregació de funcions, la gestió de privilegis, la protecció d'endpoints, la seguretat de xarxa i accés remot, la generació d'evidències, la coordinació amb Seguretat Corporativa i la col·laboració en incidents de seguretat. Aquestes funcions s'hauran de prestar sense substituir les responsabilitats pròpies dels serveis SOC, CERT o equivalents quan aquests estiguin fora de l'abast del servei.
- **Model cloud, Microsoft 365 i govern del consum:** el servei haurà d'executar l'administració, seguretat, optimització i evolució dels entorns Azure, Microsoft 365 i la resta de serveis cloud o SaaS corporatius que determini l'Agència. Aquesta característica inclou la governança cloud, etiquetatge, configuració segura, gestió d'identitats, llicenciament, control de costos, capacitat, integració, adopció de capacitats natives, optimització de consum i reducció ordenada de dependències d'infraestructura pròpia quan sigui viable i aprovat per l'Agència.
- **Model d'intel·ligència artificial i Copilot:** el servei haurà d'incorporar, quan l'Agència ho autoritzi, capacitats d'intel·ligència artificial de manera segura, governada, traçable i mesurable, incloent Microsoft 365 Copilot, Copilot Studio, Security Copilot o altres eines autoritzades. L'ús d'aquestes capacitats haurà d'estar subjecte a governança, rols, permisos, dades autoritzades, controls de seguretat, limitacions d'ús, supervisió humana, registre d'evidències i mesura del benefici operatiu. Els casos d'ús hauran d'estar validats per l'Agència i orientats a productivitat, documentació, suport al servei, automatització, anàlisi d'informació, investigació tècnica o resposta de seguretat.

- **Model de workplace digital, mobilitat i accés remot segur:** el Servei TIC haurà de contribuir a un entorn de lloc de treball digital segur, homogeni, governat i eficient per als usuaris interns i col·laboradors de l'Agència. Aquesta característica inclou la gestió de dispositius amb Intune, suport a Microsoft 365, gestió de perfils i polítiques, Azure Virtual Desktop, Prisma Browser, accés remot segur, suport a usuaris, qualitat percebuda, gestió de dispositius corporatius i BYOD quan apliqui, i traçabilitat del compliment de les polítiques corporatives.
    - **Seguretat, compliment i traçabilitat:** el servei haurà d'executar l'aplicació de les polítiques de seguretat, el compliment de l'ENS, el control d'accessos, la segregació de funcions, la gestió de privilegis, la protecció d'endpoints, la seguretat de xarxa i accés remot, la generació d'evidències, la coordinació amb Seguretat Corporativa i la col·laboració en incidents de seguretat sense substituir les funcions pròpies dels serveis SOC, CERT o equivalents fora de l'abast del Servei TIC.
    - **Model cloud, Microsoft 365 i govern del consum:** el servei haurà d'executar el model definit per administrar, assegurar, optimitzar i evolucionar l'entorn Azure, Microsoft 365 i la resta de serveis cloud o SaaS corporatius, incloent governança, etiquetatge, configuració segura, identitat, llicenciament, control de costos, capacitat, integració, adopció de capacitats natives, optimització de consum i reducció ordenada de dependències d'infraestructura pròpia quan sigui viable i aprovat per l'Agència.
- **Model d'observabilitat, monitorització i evolució cap a AIOps:** el servei haurà de disposar d'una capacitat de monitorització i observabilitat sobre els sistemes, serveis, xarxes, plataformes cloud, entorns de virtualització, còpies de seguretat, lloc de treball digital i components crítics. Aquesta capacitat haurà d'incloure supervisió contínua, gestió d'alertes, correlació, detecció d'anomalies, reducció de soroll operatiu, anàlisi de tendències, quadres de comandament, resposta automatitzada quan sigui viable i autoritzada, i evolució progressiva cap a capacitats avançades d'observabilitat i AIOps.
- **Model de backup, recuperació i continuïtat:** el servei haurà d'executar la cobertura, execució, seguiment, validació i millora de les còpies de seguretat, recuperació i continuïtat operativa dels actius i serveis gestionats. Aquesta característica inclou Cohesity, Azure Backup, entorns de virtualització, cloud i serveis crítics, així com proves de restauració, evidències de recuperabilitat, tractament d'errors, gestió de capacitat, riscos, RTO/RPO quan apliqui i coordinació amb els plans de continuïtat de l'Agència.
- **Model d'inventari, CMDB i mapa de serveis:** el servei haurà de mantenir una visió fiable, actualitzada i explotable dels actius, elements de configuració, relacions, dependències, ubicació, criticitat, titularitat i configuracions dels serveis gestionats. Aquesta informació haurà d'estar integrada, quan correspongui, amb Lansweeper, CMDB, ITSM, monitorització, seguretat, documentació i reporting, i haurà de permetre la gestió del canvi, l'anàlisi de riscos, l'aportació d'informació per al control econòmic-operatiu i el suport a la presa de decisions tècniques de l'Agència.
- **Model d'automatització, integració i orquestració:** el servei haurà de disposar d'un model d'automatització, integració i orquestració orientat a reduir intervencions manuals, minimitzar errors, millorar la qualitat de la dada, incrementar la traçabilitat i reforçar l'eficiència operativa. Aquest model haurà d'incloure automatitzacions, scripts, runbooks, fluxos, plantilles i integracions documentades, provades, versionades, segures, mantenibles i reversibles, integrades amb eines com OTRS, Zabbix, Lansweeper, Intune, Azure, Microsoft 365, Cohesity i plataformes de seguretat autoritzades.
- **Model de lliurables, KPIs i evidències:** l'adjudicatari haurà de generar, mantenir i lliurar els informes, quadres de comandament, registres, evidències, plans i documentació associats als productes, lliurables i KPIs definits en el punt 2.2.4. Aquests elements hauran de disposar de periodicitat, responsables, canals, format, criteris de qualitat, mecanismes de validació i traçabilitat suficient per permetre el seguiment contractual i el govern del servei.
- **Model de documentació i gestió del coneixement:** el servei haurà de disposar d'un model de documentació i gestió del coneixement que asseguri que tota la informació tècnica, operativa i funcional generada o mantinguda durant el contracte sigui propietat de l'Agència,

estigui actualitzada, versionada, validada, accessible i organitzada en l'entorn documental corporatiu. Aquest model haurà d'incloure procediments operatius, manuals tècnics, guies de suport, base de coneixement, inventari documental, mecanismes de revisió periòdica i transferència efectiva de coneixement.
Quan l'Agència ho determini, la documentació tècnica i operativa del servei podrà adaptar-se a formats basats en Markdown i eines de gestió del coneixement com Obsidian o equivalents, sempre integrades o coordinades amb l'ecosistema Microsoft 365 corporatiu. Tota la informació, documents, evidències i bases de coneixement hauran de romandre dins del tenant Microsoft 365 de l'Agència o dels repositoris corporatius autoritzats, especialment SharePoint, OneDrive i Teams, sense ús de repositoris paral·lels, núvols personals o entorns externs no autoritzats.

- **Model de transició, evolució tecnològica i reversibilitat:** el servei haurà de disposar d'un model de transició, evolució tecnològica i reversibilitat que asseguri l'assumpció ordenada del servei, la continuïtat durant l'arrencada, el suport a evolucions tecnològiques, migracions o substitució de plataformes, i el traspàs final del coneixement i dels actius documentals. Aquest model haurà de minimitzar riscos, dependències, pèrdua de coneixement i impacte operatiu en cas de canvi tecnològic, substitució de proveïdor o finalització contractual.
- **Model de transició postquàntica i criptoagilitat:** el servei haurà de contribuir a la preparació de la transició progressiva dels sistemes, serveis, aplicacions i plataformes de l'Agència cap a mecanismes criptogràfics resistents a la computació quàntica. Aquesta característica inclou la identificació i manteniment de l'inventari de dependències criptogràfiques, l'anàlisi dels riscos associats, l'avaluació de l'impacte sobre els serveis gestionats, la definició i manteniment actualitzat d'un full de ruta de transició postquàntica, la promoció de criteris de criptoagilitat i el seguiment dels estàndards, recomanacions i requeriments que esdevinguin aplicables durant la vigència del contracte.
- **Model de millora contínua:** el servei haurà de disposar d'un model de millora contínua basat en dades, indicadors, riscos, recurrències, desviacions, experiència d'usuari, qualitat documental, seguretat, disponibilitat, automatització, observabilitat, optimització de costos i eficiència operativa. Les accions de millora hauran de ser concretes, mesurables, verificables, amb proposta de priorització, aprovades per l'Agència i acompanyades d'evidències d'execució i benefici obtingut.
- **Model de riscos, dependències i continuïtat operativa:** el servei haurà de mantenir un model de gestió de riscos i dependències que identifiqui, registri, proposi priorització i faci seguiment dels riscos tècnics, organitzatius, de seguretat, disponibilitat, coneixement, dependència tecnològica, capacitat i transició associats a la prestació del servei. Per a cada risc rellevant s'hauran de proposar mesures de mitigació, responsables operatius, mecanismes de seguiment, estat, impacte, termini i evidències per al control de l'Agència.
- **Model de qualitat, traçabilitat i compliment del plec:** el servei haurà d'assegurar la traçabilitat entre els requeriments del plec, les activitats executades, els productes, els lliurables, els KPIs, els ANS, les evidències i el seguiment contractual. Aquesta traçabilitat haurà de permetre verificar el compliment del contracte, identificar desviacions, donar suport als comitès de seguiment i facilitar la presa de decisions operatives, tècniques i econòmiques.

Durant l'execució del contracte, l'adjudicatari haurà de mantenir una matriu de traçabilitat que relacioni objectius, activitats, productes, lliurables, KPIs, ANS i evidències del Servei TIC.

- Aquesta matriu tindrà com a finalitat facilitar el seguiment contractual, la verificació del compliment, la identificació de desviacions i la connexió entre les obligacions del plec i les evidències generades durant la prestació del servei.
- La matriu haurà d'estar permanentment actualitzada i disponible per al Servei TIC, de manera que permeti verificar, en cada moment, l'estat de compliment dels compromisos assumits per l'adjudicatari i la seva correspondència amb els resultats efectivament lliurats.
- Així mateix, haurà de permetre identificar responsabilitats, terminis, dependències, riscos associats i accions correctores o de millora derivades del seguiment del servei. Aquesta

traçabilitat haurà de facilitar també la preparació de comitès de seguiment, revisions periòdiques, auditories, justificacions contractuals i processos de transferència de coneixement, garantint una visió ordenada, coherent i verificable de l'execució del contracte.

Objectiu	Activitat o funcionalitat	Producte o lliurable	KPI de seguiment	ANS relacionat	Evidència
Objectiu estratègic o necessitat del servei a què dona resposta.	Activitat operativa, funcionalitat o procés associat.	Producte, lliurable, document, informe, registre o capacitat generada.	Indicador de seguiment, governança o millora contínua.	Codi ANS aplicable, quan correspongui.	Font, registre, informe, acta, quadre de comandament o altra evidència verificable.

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar en règim ordinari de dilluns a divendres laborables segons el calendari aplicable al centre de treball de l'Hospitalet de Llobregat.

L'adjudicatari haurà de garantir una cobertura ordinària del servei entre les 8:00 h i les 18:00 h, organitzant els recursos, torns o solapaments necessaris per cobrir aquest interval, respectant la jornada laboral i el conveni aplicable als perfils adscrits. Addicionalment, l'adjudicatari haurà d'executar el model de guàrdia establert per l'Agència per atendre incidències o necessitats crítiques relacionades amb la disponibilitat, la seguretat o la continuïtat operativa fora de l'horari ordinari de prestació.

L'adjudicatari haurà de garantir cobertura durant els dotze mesos de l'any. L'adjudicatari haurà de planificar vacances, absències, permisos o altres indisponibilitats del seu personal de manera que no es redueixi la capacitat compromesa, no es degradi el servei i no s'afecti el compliment dels ANS.

A petició expressa de l'Agència, l'adjudicatari haurà de poder executar actuacions fora de l'horari ordinari quan siguin necessàries per garantir la continuïtat, disponibilitat, seguretat o correcta evolució del servei, especialment en casos d'incidències crítiques, finestres de manteniment, actuacions planificades, canvis que puguin afectar usuaris o activitats que no es puguin executar sense impacte dins l'horari ordinari.

El servei d'alerta o guàrdia fora de l'horari ordinari s'entén com la disponibilitat necessària per rebre, analitzar, escalar i, quan correspongui, actuar sobre incidències o alertes crítiques que puguin afectar la disponibilitat, seguretat, continuïtat operativa o lloc de treball dels usuaris de l'Agència. Aquest servei s'haurà de prestar d'acord amb els criteris de prioritat, escalat, temps de resposta i canals que determini l'Agència.

L'adjudicatari haurà d'executar el model de guàrdia que determini l'Agència per garantir l'atenció d'incidències crítiques fora de l'horari ordinari de prestació, d'acord amb les franges de cobertura, canals d'activació, criteris d'activació, perfils habilitats, nivells d'escalat, temps de resposta, mecanismes de comunicació, eines d'accés remot segur, requisits de registre i evidències que aquesta determini.

L'Agència podrà revisar, actualitzar o modificar aquest model durant la vigència del contracte per adaptar-lo a les necessitats operatives, de seguretat o de continuïtat del servei. L'adjudicatari haurà de col·laborar en la seva revisió i millora contínua, aportant propostes i recomanacions quan sigui requerit, sense que això impliqui l'assumpció de funcions de definició, aprovació o governança, que corresponen exclusivament a l'Agència.

El model de guàrdia haurà de garantir la disponibilitat de perfils amb capacitat suficient per analitzar, prioritzar, escalar i actuar sobre incidències o alertes crítiques que afectin la disponibilitat, seguretat, continuïtat operativa o lloc de treball dels usuaris de l'Agència. Com a mínim, l'adjudicatari haurà de preveure cobertura funcional de coordinació del servei, infraestructura i seguretat TIC, i lloc de treball digital quan l'impacte afecti usuaris, serveis o accessos crítics.

Els perfils activables en guàrdia hauran de conèixer els procediments d'escalat, les eines ITSM i de monitorització, els entorns tecnològics sota abast, els canals de comunicació amb l'Agència, les polítiques de seguretat aplicables, els criteris de priorització i els límits d'actuació establerts per l'Agència. L'adjudicatari haurà de garantir que aquests perfils disposen dels accessos, permisos i

mitjans necessaris per actuar de manera segura, traçable i proporcional, sempre sota el principi de mínim privilegi.

La guàrdia s'activarà exclusivament davant situacions crítiques o necessitats justificades, com indisponibilitat de serveis crítics, alertes crítiques de monitorització, incidències de seguretat que afectin components TIC sota l'abast del servei, problemes greus de backup o recuperació, afectacions rellevants d'identitat, Microsoft 365, accés remot, Azure Virtual Desktop, xarxa o lloc de treball digital, o actuacions planificades fora de l'horari ordinari aprovades per l'Agència.

Cada activació de la guàrdia haurà de quedar registrada en l'eina ITSM o mecanisme que determini l'Agència, incloent hora d'activació, motiu, criticitat, perfil activat, actuacions realitzades, escalats, decisions adoptades, impacte, estat final, evidències tècniques i accions de seguiment. Aquest registre servirà com a evidència per al seguiment del servei, validació d'ANS, control de qualitat i revisió en comitès.

El model de guàrdia no substitueix les funcions pròpies dels serveis SOC, CERT, CTTI o altres proveïdors especialitzats quan aquestes estiguin fora de l'abast del Servei TIC. L'adjudicatari haurà de coordinar-se amb aquests equips o proveïdors quan la naturalesa de la incidència ho requereixi, seguint els circuits d'escalat i responsabilitat definits per l'Agència.

Les actuacions fora de l'horari ordinari hauran de ser planificades i autoritzades prèviament per l'Agència, excepte en situacions d'urgència o incidència crítica. El règim econòmic aplicable a aquestes actuacions, si escau, serà el que estableixin el contracte, el PCAP o les condicions econòmiques aprovades, sense perjudici de les actuacions que hagin d'entendre's incloses dins la cobertura ordinària del servei o del servei d'alerta. Aquest plec tècnic no determina per si mateix imports, preus unitaris ni conceptes facturables addicionals, que hauran de quedar establerts en la documentació econòmica o administrativa corresponent.

Si durant l'execució del contracte l'Agència identifica la necessitat de modificar l'horari de prestació, cobertura, règim de guàrdia o mecanismes d'atenció, aquesta modificació es tractarà de manera coordinada amb l'adjudicatari, però correspondrà a l'Agència determinar finalment el model que millor s'adeqüi a les necessitats del servei, sempre dins del marc contractual aplicable i amb criteris de proporcionalitat operativa.

3.2 Localització física

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 80% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

El mínim de dies necessaris de presencialitat a les oficines de l'Agència són 2 a la setmana, a excepció de la funció de lloc de treball que haurà de venir un mínim de 4 dies.

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.

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

L'adjudicatari haurà de disposar d'un equip de treball suficientment dimensionat i amb la qualificació adequada per garantir la correcta execució del Servei TIC, el compliment dels ANS i la continuïtat operativa del servei.

L'adjudicatari haurà de disposar dels mitjans personals necessaris per a la prestació dels serveis hauran de ser adequats per executar amb garanties les tasques definides al plec i hauran d'acreditar competències tècniques, operatives i relacionals verificables, orientades a la qualitat del servei, la seguretat, la continuïtat operativa, la documentació, la coordinació amb equips interns i externs i el compliment de les polítiques de l'Agència.

En concret, el personal haurà de demostrar:

- Professionalitat, responsabilitat, orientació a servei i respecte per les normes internes, els usuaris, els equips de treball i la informació gestionada.
- Capacitat de comunicació clara, escrita i oral, adequada tant per a interlocutors tècnics com funcionals, incloent la documentació d'actuacions, incidències, decisions i acords.
- Capacitat de treball en equip i coordinació amb l'Agència, Seguretat Corporativa, Aprovisionament, CTTI, altres proveïdors i equips interns o externs relacionats amb la prestació del servei.
- Capacitat per identificar, analitzar, prioritzar i resoldre incidències, problemes i riscos, aplicant criteris de criticitat, impacte, traçabilitat i escalat adequat.
- Capacitat per treballar sota pressió en entorns crítics, mantenint la qualitat de l'execució, la comunicació i la documentació de les actuacions.
- Coneixement suficient de català i castellà, parlat i escrit, per garantir la comunicació operativa i documental del servei, i coneixement d'anglès per a la gestió de documentació tècnica, fabricants i proveïdors tecnològics quan sigui necessari.
- Coneixement de l'entorn tecnològic, normatiu i organitzatiu aplicable al servei, incloent bones pràctiques de gestió TIC, seguretat de la informació, ENS i funcionament de l'administració pública.
- Capacitat per mantenir actualitzada la documentació, transferir coneixement, seguir procediments aprovats, complir les polítiques de seguretat i contribuir a la millora contínua del Servei TIC.

Addicionalment a l'equip mínim adscrit al servei, l'adjudicatari haurà de disposar durant tota la vigència del contracte de capacitat consultora i tècnica especialitzada suficient per donar suport al Servei TIC en aquells àmbits que requereixin coneixement expert, suport avançat o capacitats complementàries als perfils ordinaris del contracte.

Aquesta capacitat haurà de cobrir, com a mínim, els àmbits de Microsoft 365, Azure, infraestructura híbrida, identitat i accés, seguretat i compliment ENS, xarxa, virtualització, continuïtat operativa, backup, observabilitat, automatització, governança tecnològica i ús governat de tecnologies d'intel·ligència artificial.

L'ús d'aquesta capacitat especialitzada tindrà caràcter puntual, extraordinari, no recurrent i vinculat a l'abast del Servei TIC, i no podrà comportar cap reducció de les dedicacions mínimes exigides ni cap cost addicional per a l'Agència, sempre que es tracti d'activitats de suport, assessorament, revisió, escalat tècnic o validació especialitzada necessàries per a la correcta execució del servei i no de projectes singulars o prestacions addicionals fora de l'abast contractual.

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

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat de l'equip que dona servei a l'Agència. Aquesta continuïtat s'haurà de gestionar de manera coherent amb els apartats relatius al canvi de recurs, control de rotació, gestió del coneixement i documentació, assegurant la transferència efectiva de coneixement, la preservació de la qualitat del servei i el compliment dels ANS.

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **[8.800] hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Coordinador del Servei	**1.760 hores**
Enginyer d'Infraestructures i Seguretat	**1.760 hores**
Enginyer d'Infraestructures i Seguretat	**1.760 hores**
Enginyer de Lloc de Treball Modern	**1.760 hores**
Tècnic de Lloc de Treball Modern	**1.760 hores**

Els requisits anteriors s'han d'entendre com a mínims per a la prestació del servei, podent l'adjudicatari ampliar-los i millorar-los per tal de disposar de capacitat suficient per cobrir tots els àmbits funcionals del Servei TIC, garantir la continuïtat operativa i complir els Acords de Nivell de Servei (ANS) i la resta de requeriments funcionals establerts en aquest plec. Només podran haver ajustos en la distribució de dedicacions entre perfils quan estiguin degudament justificats i no impliquin una reducció de la capacitat global del servei, de la qualitat esperada ni del compliment dels ANS.

Aquest dimensionament té per finalitat assegurar la capacitat mínima necessària per a la correcta prestació del Servei TIC i no implica, en cap cas, una cessió de personal, una adscripció funcional directa a l'Agència ni una obligació de dedicació exclusiva de persones concretes. L'organització, direcció, planificació, supervisió laboral, assignació de tasques internes, cobertura d'absències i gestió del personal correspon exclusivament a l'adjudicatari, sense perjudici de les facultats de seguiment, validació, control del compliment contractual i verificació de resultats que corresponen a l'Agència.

L'adjudicatari haurà de disposar de capacitat per absorbir pics de demanda, incidències crítiques, increments puntuals d'activitat o necessitats derivades de projectes i evolucions tecnològiques, sense degradar la prestació ordinària del servei. L'adjudicatari haurà de disposar d'un mecanisme de reforç temporal, escalat intern, suport expert o redistribució controlada de capacitat, així com els criteris que permetran revisar el dimensionament quan la demanda superi de manera sostinguda els llindars previstos.

En el cas dels dos perfils d'Enginyer d'Infraestructures i Seguretat previstos a la taula de dimensionament, aquests podran aportar capacitats complementàries sempre que, de manera conjunta, cobreixin tots els requisits funcionals i tècnics exigits per al perfil.

En cap cas la participació del personal assignat per l'adjudicatari en la prestació del Servei TIC comportarà relació laboral, dependència jeràrquica, integració organitzativa ni exercici de facultats empresarials per part de l'Agència. Les instruccions de l'Agència tindran naturalesa estrictament contractual, funcional i de seguiment del servei, i s'adreçaran a l'adjudicatari o als interlocutors designats, sense perjudici de les interaccions operatives necessàries per a la correcta execució, coordinació i traçabilitat de les activitats.

3.4 Perfils

Els coneixements i competències tècniques definits per a cada perfil tenen caràcter de requisit funcional mínim, en la mesura necessària per cobrir les activitats del servei.

Les certificacions, fabricants, plataformes o tecnologies esmentades en aquest apartat s'han d'entendre sempre referides a l'ecosistema tecnològic existent o previst de l'Agència i tindran caràcter funcional o valorable segons correspongui, admetent-se certificacions, formacions, experiències o acreditacions equivalents que permetin demostrar competències tècniques suficients per executar les funcions requerides.

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

PERFIL	REQUISITS
Coordinador del Servei	**Coneixements i competències tècniques:** • Govern operatiu i coordinació integral de serveis de suport tècnic, amb capacitat per organitzar l'execució diària, coordinar els diferents perfils del servei, assegurar la cobertura funcional dels àmbits contractats i garantir l'alineament amb les directrius, prioritats i decisions de l'Agència. • Seguiment global de contractes de servei, dels Acords de Nivell de Servei, KPIs, lliurables, riscos, desviacions, plans d'acció, qualitat documental, control de capacitat i evidències de compliment, aportant informació fiable i traçable per al govern del servei. • Gestió de la relació operativa, incloent la preparació i participació en comitès de seguiment, la coordinació d'escalats, el seguiment de compromisos, la gestió de dependències amb altres departaments, entitats, proveïdors i equips interns, i la comunicació estructurada de l'estat del servei. • Coneixement funcional transversal dels àmbits d'infraestructura, cloud, workplace, identitat, xarxa, seguretat, monitorització, ITSM, CMDB, documentació, automatització, continuïtat i governança tecnològica, suficient per coordinar l'execució, validar l'adequació operativa, identificar riscos i activar els escalats corresponents, sense substituir els perfils especialistes ni les funcions de decisió. • Capacitat per impulsar la millora contínua del servei, la qualitat de la informació, la reducció de dependències individuals, la transferència de coneixement, l'automatització de processos, la revisió de recurrències i la preparació de propostes de millora per a la seva validació. **Aptituds i habilitats:** • Capacitat de lideratge operatiu, coordinació transversal, priorització i gestió de càrrega de treball en entorns crítics, híbrids i multidomini.

- Orientació a servei, disponibilitat, seguretat, qualitat, traçabilitat i compliment contractual, amb capacitat per anticipar desviacions i activar mesures correctores.
- Comunicació executiva i operativa clara amb equips tècnics, responsables de servei, òrgans de seguiment i altres interlocutors, transformant informació tècnica i operativa en informació útil per a la presa de decisions.
- Rigor en el seguiment de compromisos, documentació, reporting, manteniment d'evidències, gestió d'actes, control de riscos i transferència de coneixement.
- Proactivitat, capacitat de treball sota pressió, criteri per gestionar escalats i incidències crítiques, i orientació a la millora contínua i a l'eficiència operativa del servei.

Formació i coneixements mínims exigibles:

- Grau en Enginyeria Informàtica, Telecomunicacions o àmbits similars, o titulació equivalent adequada a la funció de coordinació i govern operatiu de serveis TIC.
- 5 anys d'experiència recent i acreditable en coordinació de serveis TIC gestionats, recurrents i multidisciplinaris, amb responsabilitat sobre la planificació, seguiment, control de qualitat, coordinació operativa i gestió d'incidències, peticions, canvis, problemes i escalats.
- Experiència en gestió ITSM, seguiment d'ANS, priorització de la demanda, gestió de capacitat, millora contínua i control de riscos operatius vinculats a disponibilitat, seguretat i continuïtat.
- Capacitat d'interlocució amb responsables de l'organització, coordinació transversal amb unitats internes, equips tècnics, seguretat, aprovisionament i proveïdors, així com elaboració de reporting operatiu i executiu.
- Capacitat per garantir la qualitat, actualització i traçabilitat de la documentació del servei, incloent procediments, runbooks, informes, actes, plans d'acció i transferència de coneixement.
- Coneixement funcional suficient dels àmbits d'infraestructura, cloud, xarxa, seguretat, workplace, monitorització, automatització, observabilitat, continuïtat i coordinació operativa necessaris per al rol.
- Certificació ITIL Foundation o superior, o acreditació equivalent en gestió de serveis TIC.
- Certificació Microsoft AZ-900 o equivalent.

Certificacions i formacions valorables:

- Certificacions o formació en governança, qualitat, gestió de serveis, ISO/IEC 20000, ISO/IEC 27001, ENS, gestió de riscos, continuïtat de negoci o marcs equivalents.
- Certificacions o formació en govern, administració i seguretat d'entorns empresarials de Microsoft o altres clouds, amb enfocament de govern i coordinació del servei.

	• Formació en reporting, control de gestió, gestió de contractes TIC, quadres de comandament, automatització, integració, observabilitat o millora operativa. • Coneixement d'anglès suficient per gestionar documentació tècnica, relació amb fabricants, proveïdors tecnològics i informació associada a plataformes empresarials.
Enginyer d'Infraestructures i Seguretat	**Coneixements i competències tècniques:** • Administració d'infraestructura híbrida, cloud, sistemes, virtualització i hiperconvergència, assegurant disponibilitat, escalabilitat, seguretat i continuïtat dels serveis gestionats. • Operació de xarxa corporativa, segmentació, connectivitat, integració amb entorns cloud i serveis crítics, incloent la resolució d'incidències complexes i la coordinació amb altres equips. • Gestió de seguretat perimetral, accés segur, endpoint, identitat, models Zero Trust i compliment ENS, sense substituir les funcions pròpies dels serveis SOC/CERT quan siguin fora de l'abast del Servei TIC. • Gestió de backup, recuperació, continuïtat, monitorització, observabilitat i operació d'entorns crítics, amb capacitat per generar evidències i propostes de millora. • Automatització, scripting, integració amb ITSM/CMDB, documentació tècnica i aplicació de bones pràctiques de seguretat i gestió TIC. **Aptituds i habilitats:** • Capacitat d'anàlisi i resolució tècnica d'incidències complexes en entorns híbrids, crítics i multitecnologia. • Visió d'extrem a extrem sobre infraestructura, xarxa, seguretat, backup, continuïtat i dependències entre serveis. • Proactivitat per detectar riscos, millores d'arquitectura, optimitzacions operatives i oportunitats d'automatització. • Rigor en la documentació tècnica, generació d'evidències, aplicació de procediments i escalat coordinat amb altres perfils. • Capacitat de treball sota pressió, coordinació amb equips tècnics i ús d'anglès tècnic per a documentació i proveïdors. **Formació i coneixements mínims exigibles:** • Grau en Enginyeria Informàtica, Telecomunicacions o àmbits similars. • 3 anys d'experiència recent i acreditable en administració d'infraestructures híbrides, sistemes, xarxa, seguretat, virtualització, backup o continuïtat operativa. • Coneixement funcional suficient dels entorns d'infraestructura local i cloud, xarxa, seguretat, monitorització, automatització, backup, recuperació i compliment ENS necessaris per al perfil. • Coneixement funcional suficient d'infraestructura local i cloud, xarxa, identitat, seguretat perimetral i endpoint, còpies de seguretat, recuperació, automatització, observabilitat i compliment ENS necessaris per al perfil. • Certificacions Microsoft Azure Administrator Associate o equivalent.

	• Certificació Cisco CCNA o equivalent en xarxes. • Certificació Palo Alto Networks PCNSA o equivalent en seguretat. **Certificacions i formacions valorables:** • Azure Solutions Architect Expert • Azure Security Engineer • CCNP • Palo Alto PCNSE • Nutanix NCP • VMware VCP • CISSP • CISM • Cohesity
Enginyer de Lloc de Treball Modern	**Coneixements i competències tècniques:** • Administració de Microsoft 365, Exchange Online, Teams, SharePoint, OneDrive i serveis associats, garantint una experiència d'usuari segura, eficient i alineada amb les polítiques corporatives. • Gestió d'identitat, accessos, dispositius i polítiques amb Entra ID i Intune, incloent configuració, compliment, seguretat, actualitzacions i govern del parc de dispositius. • Gestió de Windows 10/11, suport L2, endpoint, seguretat del lloc de treball, llicenciament i compliment, amb capacitat per diagnosticar incidències recurrents i proposar millores. • Gestió d'accés remot segur, Azure Virtual Desktop o equivalents, mobilitat, teletreball segur i qualitat de l'experiència d'usuari. • Automatització, integració amb ITSM/CMDB, documentació operativa i millora contínua del workplace digital. **Aptituds i habilitats:** • Orientació a l'usuari i a la qualitat de l'experiència digital, amb comunicació clara amb perfils tècnics i no tècnics. • Capacitat de diagnòstic, priorització i resolució d'incidències workplace, dispositius, identitat i accés remot. • Proactivitat per detectar recurrències, millores de configuració, automatitzacions i oportunitats d'optimització del lloc de treball. • Rigor en la documentació de procediments, incidències, solucions, polítiques i evidències de compliment. • Capacitat de coordinació amb infraestructura, xarxa, seguretat i suport, amb adaptabilitat a l'evolució de les eines Microsoft i anglès tècnic suficient. **Formació i coneixements mínims exigibles:** • Grau en Enginyeria Informàtica, Telecomunicacions o àmbits similars. • 3 anys d'experiència recent i acreditable en gestió de lloc de treball digital, Microsoft 365, Intune, identitat, suport L2, dispositius, accés remot i seguretat endpoint. • Experiència en configuració, administració, desplegament, suport, diagnòstic, resolució d'incidències, gestió de canvis i millora contínua de serveis de lloc de treball modern.

	• Microsoft 365 Endpoint Administrator Associate (MD-102 o equivalent vigent) **Certificacions i formacions valorables:** • Microsoft 365 Administrator Expert • Identity and Access Administrator • Security Operations Analyst • Defender • Power Platform • Copilot • Copilot Studio
Tècnic de Lloc de Treball Modern	**Coneixements i competències tècniques:** • Suport a usuaris i resolució d'incidències de Microsoft 365, Windows, dispositius, aplicacions corporatives i eines de col·laboració. • Suport bàsic a identitat, accessos, dispositius, perifèrics, connectivitat, accés remot i configuracions habituals del lloc de treball digital. • Ús d'eines ITSM per registrar, categoritzar, seguir, documentar i tancar incidències i peticions, assegurant qualitat del registre i traçabilitat. • Aplicació de procediments operatius, bones pràctiques de seguretat, documentació de solucions i escalat ordenat cap a perfils tècnics superiors quan sigui necessari. • Suport a la gestió de llicències, inventari, dispositius i millores bàsiques del servei de lloc de treball. **Aptituds i habilitats:** • Orientació a l'atenció a l'usuari, qualitat del suport i comunicació clara amb perfils tècnics i no tècnics. • Capacitat de gestionar incidències i peticions simultànies, prioritzant segons criticitat, impacte i procediments establerts. • Rigor en el registre ITSM, documentació de solucions, seguiment de tiquets i escalat cap a perfils tècnics superiors. • Proactivitat per detectar recurrències, aplicar bones pràctiques de seguretat i contribuir a la millora dels processos de suport. • Treball en equip, adaptabilitat a eines de workplace digital i anglès bàsic o intermedi per comprendre documentació tècnica. **Formació i coneixements mínims exigibles:** • Cicle formatiu de grau mitjà o superior en informàtica, telecomunicacions o àmbits similars. • 2 anys d'experiència recent i acreditable en suport TIC a usuaris, Microsoft 365, Windows, dispositius, eines ITSM, gestió d'incidències i aplicació de bones pràctiques de seguretat. • Experiència en atenció a usuaris, diagnòstic inicial, escalat, resolució d'incidències, suport a dispositius, configuració bàsica, documentació d'actuacions i seguiment de peticions. • Coneixement funcional suficient del suport al lloc de treball digital, resolució d'incidències, configuració bàsica de dispositius, registre de tiquets, documentació operativa i atenció a usuaris.

	Certificacions i formacions valorables: • MD-102 • MS-900 • ITIL Foundation • Formació Microsoft 365 • Formació Intune

Als efectes de la valoració econòmica, únicament es tindran en compte els perfils inclosos a la taula de dimensionament del servei. La resta de perfils definits al plec o aportats pel servei com a suport especialitzat es consideraran part de l'estructura del proveïdor i no seran objecte de facturació directa.

3.5 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari el canvi d'un recurs que depengui d'aquest quan ho requereixi la correcta execució dels treballs, la qualitat del servei, el compliment dels requisits exigits per als perfils, la seguretat, la disponibilitat, la continuïtat operativa, el dimensionament o l'organització del Servei TIC. Aquesta exigència podrà fonamentar-se, entre d'altres, en manca d'adequació tècnica, incompliment de procediments, baixa qualitat recurrent, manca de documentació, problemes de coordinació, indisponibilitat reiterada, incompliments d'ANS atribuïbles al recurs, risc de seguretat o manca d'adaptació a les eines, metodologies i polítiques de l'Agència.

La substitució s'haurà de fer efectiva en un termini màxim de 15 dies laborables a partir de la comunicació de l'Agència. En situacions de risc operatiu, de seguretat o d'incompliment greu, l'Agència podrà requerir la retirada immediata del recurs de determinades funcions, accessos o activitats, així com una substitució urgent en un termini compatible amb la criticitat del servei.

L'adjudicatari haurà de presentar, en un termini màxim de 10 dies laborables des de la comunicació de la sol·licitud de substitució, un pla d'acció que identifiqui les causes, les mesures correctores, el calendari, el responsable, el mecanisme de seguiment i les accions previstes per evitar la recurrència. El recurs substitut haurà d'acreditar requisits equivalents o superiors als del recurs substituït i la seva incorporació efectiva quedarà subjecta a la validació prèvia de l'Agència.

En tots els casos, el canvi de recurs no suspendrà els ANS, no eximirà l'adjudicatari de les seves responsabilitats contractuals i no podrà comportar cap cost addicional per a l'Agència. L'adjudicatari haurà de garantir el traspàs de coneixement, l'actualització de la documentació, la continuïtat de les tasques obertes i la preservació de la qualitat del servei, d'acord amb els apartats relatius a control de rotació, gestió del coneixement i documentació.

3.6 Control de rotació

L'estabilitat dels recursos del servei, el manteniment del coneixement i el compromís amb la prestació són factors crítics per garantir la continuïtat operativa, la qualitat del servei, la seguretat i el compliment dels ANS.

La identificació dels perfils crítics del servei és necessària per aplicar de manera objectiva els ANS vinculats a la continuïtat de l'equip, la rotació no planificada, la disponibilitat del personal compromès, la transferència de coneixement i la cobertura funcional equivalent. Aquesta definició permet determinar quan la substitució, absència o indisponibilitat d'un recurs pot afectar la seguretat, la

disponibilitat, la continuïtat operativa, el compliment dels ANS, la qualitat documental o la capacitat de resposta davant incidències crítiques.

S'entendrà per **perfil crític del servei** qualsevol perfil assignat al Servei TIC que concentri coneixement, responsabilitat operativa, accés, capacitat tècnica o interlocució rellevant que no pugui ser coberta de manera immediata, segura i equivalent per qualsevol altre perfil del servei sense impacte en la seguretat, disponibilitat, continuïtat operativa, compliment dels ANS, qualitat documental o capacitat de resposta davant incidències crítiques.

L'adjudicatari podrà proposar canvis en l'equip de treball durant l'execució del contracte per causes degudament justificades, com ara baixa, rotació interna, reorganització, finalització de relació laboral o altres circumstàncies alienes a l'Agència. Aquests canvis hauran de ser notificats per escrit a l'Agència amb una antelació mínima de 14 dies naturals, indicant el motiu del canvi, el perfil afectat, la data prevista de sortida, la persona proposada com a substituta, la seva qualificació, experiència, dedicació prevista i cobertura funcional. La incorporació efectiva del recurs substitut quedarà subjecta a la validació prèvia de l'Agència, que podrà rebutjar-lo si no acredita requisits equivalents o superiors als del perfil substituït o si no resulta adequat per garantir la correcta prestació del servei.

L'adjudicatari assumirà la selecció de les persones de nova incorporació i haurà de garantir la coexistència ordenada entre el personal sortint i entrant quan sigui necessària per assegurar el traspàs efectiu de coneixement. Aquest traspàs haurà de formalitzar-se mitjançant un pla de traspàs que inclogui, com a mínim, relació de serveis, actius, eines, procediments i responsabilitats associades al recurs sortint, estat de tasques obertes, incidències o riscos pendents, documentació actualitzada, sessions de transferència, evidències del traspàs i validació per part del Coordinador Tècnic i de l'Agència. El període de traspàs i adaptació no podrà superar, amb caràcter ordinari, els 15 dies naturals, llevat que l'Agència autoritzi expressament un termini diferent per raons justificades.

La coexistència, adaptació, formació interna, traspàs de coneixement i qualsevol dedicació necessària per garantir la continuïtat del servei no suposaran cap increment de cost ni facturació addicional per a l'Agència respecte del dimensionament ordinari del servei. En cap cas la substitució de personal podrà afectar negativament la prestació del servei, suspendre els ANS o eximir l'adjudicatari de les seves responsabilitats contractuals. L'adjudicatari haurà de garantir igualment la cobertura de les absències temporals per vacances, baixes, permisos, indisponibilitats puntuals o altres circumstàncies, mitjançant substitució, cobertura funcional, redistribució controlada de capacitat o activació de suport intern, sense degradació del servei ni cost addicional. La rotació excessiva, especialment quan afecti perfils crítics, generi pèrdua de coneixement, impacti en la qualitat, incrementi incidències, redueixi la documentació o afecti el compliment dels ANS, podrà donar lloc a l'aplicació dels mecanismes de seguiment, correcció o penalització previstos en el contracte i en els ANS aplicables.

3.7 Eines i equipament per a la prestació de serveis

Les principals plataformes, subscripcions, eines, aplicatius, entorns corporatius i accessos lògics o físics necessaris per a la prestació del servei seran proporcionats o determinats per l'Agència. L'adjudicatari haurà d'utilitzar-los exclusivament per a l'execució de les tasques derivades del Servei TIC, d'acord amb les polítiques, procediments i autoritzacions establertes per l'Agència, sense extreure, copiar, emmagatzemar, manipular o tractar informació fora de l'àmbit autoritzat sense aprovació prèvia i expressa. Qualsevol tractament temporal d'informació fora dels entorns corporatius autoritzats haurà de ser excepcional, justificat, expressament autoritzat per l'Agència, limitat al mínim necessari, protegit mitjançant controls adequats, registrat i subjecte a retorn, eliminació segura o destrucció amb evidències quan finalitzi la necessitat del tractament.

L'accés a les eines, dades i entorns de l'Agència haurà de basar-se en identitats nominals, principi de mínim privilegi, segregació de funcions, traçabilitat, registre d'activitat, revisió periòdica

d'accessos i revocació immediata quan finalitzi la participació d'un recurs o quan així ho requereixi l'Agència. L'adjudicatari haurà de col·laborar en la gestió d'altes, baixes, modificacions i revisions d'accessos, aportant les evidències que siguin requerides.

L'adjudicatari podrà identificar i proposar la incorporació d'eines que permetin millorar el servei, especialment en els àmbits d'automatització, observabilitat, optimització operativa, integració, analítica avançada o intel·ligència artificial. Qualsevol eina proposada haurà de ser aprovada prèviament per l'Agència i quedarà subjecta a validació de seguretat, privacitat, protecció de dades, compliment de l'ENS, arquitectura, interoperabilitat, llicenciament, cost total, titularitat i accés a les dades, ubicació i tractament de la informació, traçabilitat, auditoria i reversibilitat. No es podrà utilitzar cap eina SaaS, servei cloud extern, component d'intel·ligència artificial o mecanisme d'automatització amb accés a informació de l'Agència sense autorització expressa.

En relació amb les capacitats d'intel·ligència artificial, l'ús de Microsoft 365 Copilot, Copilot Studio, Security Copilot o eines equivalents haurà de ser aprovat, governat i configurat per l'Agència. L'adjudicatari només podrà utilitzar aquestes capacitats en els casos d'ús autoritzats, amb identitats nominals, permisos adequats, traçabilitat, supervisió humana i respecte estricte a les polítiques de seguretat, privacitat, protecció de dades, classificació de la informació, DLP, retenció i auditoria del tenant Microsoft 365 corporatiu.

Qualsevol eina documental, de gestió del coneixement o de suport a la creació de continguts tècnics, incloent eines basades en Markdown, Obsidian o equivalents, haurà d'estar autoritzada per l'Agència i haurà d'utilitzar-se de manera compatible amb el tenant Microsoft 365 corporatiu, sense extreure ni mantenir informació de l'Agència en repositoris, serveis o entorns no autoritzats.

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

- Ubicació física adequada per al desenvolupament i prestació dels serveis quan sigui requerida la presència a les instal·lacions de l'Agència.
- Connectivitat corporativa controlada, accés als entorns autoritzats i infraestructura de xarxa necessària per a la prestació del servei a les instal·lacions de l'Agència, d'acord amb les polítiques de seguretat i accés vigents.
- Mecanismes d'autenticació, autorització i accés als serveis corporatius necessaris per a l'execució de les funcions assignades, sempre amb caràcter nominal, traçable i restringit.
- Accés a Internet o als recursos corporatius a través dels canals i xarxes autoritzats per l'Agència, restringit als usos, ubicacions, serveis i destinacions necessaris per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula ni ordinadors portàtils.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Connectivitat mòbil o externa pròpia de l'adjudicatari, excepte quan el contracte estableixi expressament una altra cosa.
- Cap altre recurs no especificat explícitament.
- En conseqüència, l'adjudicatari haurà de:Disposar i mantenir, sota la seva responsabilitat, tots els elements necessaris per a la correcta prestació del Servei TIC que no siguin proporcionats expressament per l'Agència, incloent el maquinari, sistemes operatius, programari, connectivitat, comunicacions, equipament auxiliar i serveis de suport associats.

- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Garantir que qualsevol informació de l'Agència tractada des d'equipament propi de l'adjudicatari resti protegida, segregada i accessible només pels canals autoritzats, i que, en cas de finalització del servei, canvi de recurs o revocació d'autoritzacions, es procedeixi a la baixa d'accessos i a l'eliminació o retorn de qualsevol informació local autoritzada, amb les evidències corresponents.
- Accedir als entorns i dades de l'Agència preferentment mitjançant entorns corporatius controlats, com Azure Virtual Desktop, Prisma Browser o solucions equivalents que determini l'Agència, reduint la necessitat d'administrar, maquetar o controlar físicament dispositius propis de l'adjudicatari. L'Agència podrà establir controls de postura, requisits de seguretat del dispositiu d'origen, restriccions de descàrrega, bloqueig o revocació d'accessos i supervisió de l'activitat dins dels entorns corporatius autoritzats.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar canvis en les eines, plataformes, canals d'accés, mecanismes de seguretat i tecnologies utilitzades per a l'execució del servei. Aquests canvis hauran de ser assumits per l'adjudicatari dins del marc del contracte, garantint la continuïtat operativa i la correcta adaptació de l'equip.

Per aquest motiu, l'adjudicatari haurà de tenir presents les següents consideracions relatives a l'evolució tecnològica, la transició entre eines i l'adaptació operativa durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol nova tecnologia, eina, plataforma, servei cloud, mecanisme d'accés segur o evolució de les capacitats existents relacionades amb la prestació del servei. L'Agència decidirà la forma d'implantar aquests nous sistemes, la planificació dels projectes corresponents, el calendari, els criteris de validació, els mecanismes de transició des dels sistemes existents i les condicions de seguretat, governança i continuïtat associada.
- L'adjudicatari es compromet a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, participant activament en el procés de transició, actualitzant procediments, documentació i integracions quan sigui necessari, revisant els controls de seguretat aplicables, donant suport a proves i validacions, i formant i preparant el seu personal sense cost addicional per a l'Agència.

3.8 Gestió del coneixement

Amb l'objectiu de garantir la continuïtat operativa, la qualitat del servei, la preservació del coneixement crític i la capacitat de l'Agència per governar i evolucionar el Servei TIC, l'adjudicatari haurà de gestionar de manera estructurada, actualitzada, accessible i reutilitzable tot el coneixement tècnic, operatiu i funcional existent o generat durant l'execució del contracte. Aquesta gestió del coneixement haurà d'estar alineada amb els productes, lliurables i KPIs definits al punt 2.2.4 i amb el model de documentació i gestió del coneixement definit al punt 2.2.5.

Tot el coneixement generat, documentat o actualitzat en el marc del contracte serà propietat de l'Agència i haurà d'estar disponible en qualsevol moment en l'entorn documental corporatiu que aquesta determini. L'adjudicatari haurà de garantir que la informació estigui organitzada, versionada, validada, actualitzada, classificada, accessible per als perfils autoritzats i preparada per facilitar la transferència de coneixement, la reversibilitat, la substitució de recursos, la integració amb altres equips i la presa de decisions tècniques, operatives i de governança.

Als efectes d'aquest contracte, s'entendrà per documentació crítica aquella documentació tècnica, operativa, funcional, de seguretat o de governança indispensable per garantir la correcta prestació del Servei TIC, la continuïtat operativa, la seguretat de la informació, la transferència de coneixement, el compliment dels ANS i la reversibilitat del servei.

Com a mínim, tindran la consideració de documentació crítica:

- Arquitectures i diagrames d'alt nivell dels serveis sota abast.
- Procediments operatius i runbooks.
- Procediments de recuperació i continuïtat.
- Procediments d'administració i operació de plataformes crítiques.
- Procediments de gestió d'incidents, problemes, canvis i escalats.
- Inventaris d'actius i informació necessària per al manteniment de la CMDB.
- Configuracions bàsiques i documentació de referència d'infraestructures, sistemes i serveis crítics.
- Documentació relativa a identitats, accessos privilegiats i mecanismes d'autenticació.
- Documentació de les automatitzacions, scripts, integracions i runbooks operatius vigents.
- Plans de continuïtat, contingència, transició i reversibilitat.
- Procediments vinculats al compliment normatiu, ENS i requeriments de Seguretat Corporativa.
- Qualsevol altra documentació que l'Agència classifiqui formalment com a crítica.

Per garantir el compliment d'aquest requeriment, l'adjudicatari haurà de definir, mantenir i executar un model de gestió del coneixement que inclogui, com a mínim, les accions següents:

- **Govern del coneixement i inventari documental**
  - **Inventari del coneixement existent i generat:** elaborar i mantenir un inventari documental que identifiqui procediments operatius, manuals tècnics, guies de suport, articles de base de coneixement, runbooks, scripts, models d'informe, registres, decisions tècniques, lliurables, evidències i qualsevol altre actiu documental rellevant del Servei TIC.
  - **Estructura, taxonomia i classificació:** definir una estructura documental clara, amb categories, responsables, criticitat, estat, àmbit funcional, data d'actualització, versió, periodicitat de revisió i relació amb els productes, lliurables i KPIs del Servei TIC.
  - **Qualitat documental:** garantir que la documentació sigui clara, completa, vigent, reutilitzable, coherent amb els procediments aprovats, alineada amb les polítiques de seguretat i suficient per permetre l'operació, suport, auditoria, revisió i transferència del servei.

- **Repositori corporatiu i accés al coneixement**
  - **Repositori documental i base de coneixement:** mantenir la documentació en el repositori corporatiu que determini l'Agència, integrant-hi procediments operatius, manuals tècnics, guies de suport, preguntes freqüents, lliçons apreses, runbooks, documentació d'automatitzacions, informes, evidències i materials de transferència de coneixement.
  - **Accés, permisos i traçabilitat:** assegurar que l'Agència pugui accedir al coneixement en qualsevol moment, amb permisos adequats, control d'accessos, traçabilitat de canvis, historial de versions i capacitat d'auditoria sobre la documentació generada o mantinguda.
  - **Model Markdown i eines de gestió del coneixement:** quan l'Agència ho determini, la documentació tècnica, procedimental i operativa podrà elaborar-se o mantenir-se en formats lleugers, oberts, llegibles, versionables i reutilitzables, incloent Markdown, per facilitar la navegació entre continguts, el manteniment incremental, la reutilització del coneixement, el control de versions i la reversibilitat. Aquest model haurà d'estar sempre alineat amb l'ecosistema Microsoft 365 corporatiu de l'Agència. Tota la informació, documentació, fitxers, evidències, bases de coneixement i materials generats o mantinguts en el marc del contracte hauran de residir en tot moment dins del tenant Microsoft 365 de l'Agència o en els repositoris corporatius autoritzats que

aquesta determini, especialment SharePoint, OneDrive, Teams o serveis equivalents aprovats per l'Agència.
    - **Ús d'Obsidian o eines equivalents:** l'ús d'eines de gestió del coneixement com Obsidian o equivalents s'haurà d'entendre com un mecanisme de creació, estructuració, navegació i reutilització del coneixement, però no podrà substituir els repositoris corporatius autoritzats ni generar còpies o repositoris paral·lels fora del control de l'Agència. No es podrà mantenir informació de l'Agència en repositoris locals no autoritzats, núvols personals, serveis externs, sincronitzacions fora del tenant o entorns documentals paral·lels.

- **Actualització, validació i revisió periòdica**
    - **Actualització contínua:** actualitzar la documentació quan es produeixin canvis en sistemes, eines, configuracions, procediments, automatitzacions, integracions, processos ITSM, inventari, CMDB, monitorització, seguretat, backup, workplace, cloud o qualsevol altre àmbit funcional del Servei TIC.
    - **Validació i revisions periòdiques:** establir un calendari de revisió periòdica de la documentació crítica, amb validació per part del Coordinador del Servei, quan correspongui, de l'Agència. Les revisions hauran de generar evidències de vigència, qualitat, aprovació, obsolescència detectada i accions de correcció.

- **Transferència de coneixement i continuïtat operativa**
    - **Transferència interna i cap a l'Agència:** planificar i executar sessions de transferència de coneixement quan es produeixin canvis de recurs, rotació, incorporació de nous perfils, evolucions tecnològiques, migracions, modificacions rellevants de servei o a petició de l'Agència.
    - **Plans i evidències de traspàs:** generar plans de transferència de coneixement, actes de sessió, materials de suport, registres d'assistència, relació de continguts transferits i evidències de validació que permetin acreditar la correcta assimilació del coneixement.

- **Coordinació, seguiment i millora del coneixement**
    - **Alineació amb l'Agència i directrius corporatives:** assegurar que la gestió del coneixement s'ajusta a les directrius de l'Agència, als criteris documentals corporatius, als requeriments de seguretat, al model de lliurables del punt 2.2.4 i al model de documentació i gestió del coneixement del punt 2.2.5.
    - **Seguiment, indicadors i millora contínua:** informar periòdicament de l'estat del repositori, grau d'actualització de la documentació crítica, documents pendents de validació, articles incorporats a la base de coneixement, revisions realitzades, desviacions detectades i accions de millora associades. Aquest seguiment haurà de permetre alimentar els KPIs definits al punt 2.2.4 i els informes de govern del servei.

La gestió del coneixement haurà de considerar-se una activitat recurrent del servei i no una actuació puntual o finalista. En conseqüència, l'adjudicatari haurà de mantenir el repositori documental i la base de coneixement actualitzats durant tota la vigència del contracte, especialment després de canvis, incidències rellevants, automatitzacions, noves integracions, modificacions d'arquitectura, substitucions de personal, auditories, proves de continuïtat, actuacions de seguretat o millores aprovades.

L'incompliment recurrent de les obligacions de documentació, actualització, transferència de coneixement o qualitat documental podrà ser considerat una desviació del servei i donar lloc als mecanismes de seguiment, correcció o penalització que prevegi el contracte, especialment quan afecti la continuïtat operativa, la substitució de recursos, la reversibilitat, la seguretat, la traçabilitat o el compliment dels ANS.

3.9 Seguretat Corporativa

Un cop adjudicat el contracte, l'adjudicatari, el seu personal i, si escau, qualsevol subcontractista o tercer que participi en la prestació del servei hauran de sotmetre's a les polítiques, normes, procediments, instruccions i controls establerts per l'àrea de Seguretat Corporativa de l'Agència, així com al marc normatiu aplicable en matèria de seguretat de la informació, protecció de dades, ciberseguretat i compliment, incloent l'ENS, la normativa interna de l'Agència i qualsevol altra disposició aplicable durant la vigència del contracte.

L'adjudicatari haurà de garantir que totes les activitats, accessos, eines, dispositius, entorns, automatitzacions, integracions, documentació i tractaments d'informació vinculats al Servei TIC es realitzen d'acord amb els principis de seguretat per disseny, mínim privilegi, segregació de funcions, traçabilitat, necessitat de conèixer, control d'accés, registre d'activitat, confidencialitat, integritat, disponibilitat i reversibilitat.

L'ús d'intel·ligència artificial, incloent Microsoft 365 Copilot, Copilot Studio, Security Copilot o eines equivalents, haurà de respectar els principis de governança responsable de la IA, seguretat per disseny, privacitat des del disseny, mínima exposició de dades, supervisió humana, explicabilitat suficient, no ús de dades fora dels entorns autoritzats, absència de decisions automàtiques no autoritzades i registre de les actuacions rellevants quan sigui aplicable.

L'adjudicatari haurà d'aplicar els principis de seguretat per disseny en totes les activitats sota el seu abast. Les principals obligacions de seguretat són:

- Permetre, facilitar i col·laborar en la realització d'auditories, revisions, verificacions tècniques i controls de compliment impulsats per Seguretat Corporativa, per l'Agència o per tercers autoritzats, aportant la informació, evidències, registres, traçabilitat i plans d'acció que siguin requerits.
- Facilitar l'accés de l'Agència a la informació, evidències, registres, traces, configuracions, inventaris, documentació i entorns vinculats a la prestació del servei, sempre dins l'àmbit autoritzat i amb les garanties de seguretat i confidencialitat corresponents.
- Acceptar, aplicar i fer complir les polítiques, normes, procediments, instruccions i controls de Seguretat Corporativa des de la incorporació al servei, després de qualsevol canvi rellevant i sempre que l'Agència actualitzi el seu marc normatiu o operatiu.
- Sotmetre els accessos, dispositius d'origen, entorns corporatius, comptes, credencials, rols i permisos utilitzats per a la prestació del servei als controls de seguretat que determini l'Agència, incloent revisió periòdica, revocació immediata, restriccions de descàrrega, requisits de postura, supervisió dins dels entorns autoritzats i aplicació de polítiques corporatives.
- Garantir que la informació de l'Agència no s'emmagatzema, copia, tracta, trasllada o conserva fora dels entorns i canals autoritzats, excepte autorització expressa, i que qualsevol informació local autoritzada resta protegida, segregada, inventariada i subjecta a retorn, eliminació segura o destrucció amb evidències quan finalitzi la necessitat del tractament.
- Garantir l'estabilitat dels equips i reduir al mínim la rotació de personal, d'acord amb el model de control de rotació, traspàs de coneixement, documentació i continuïtat operativa definit en aquest plec.
- Donar compliment a totes les normes, polítiques, marcs reguladors i obligacions vigents durant el període del contracte, incloent l'ENS, RGPD, LOPDGDD, LSSI, normativa interna de l'Agència, instruccions de Seguretat Corporativa i qualsevol altra normativa aplicable a la prestació del servei.
- Comunicar de manera immediata a l'Agència qualsevol incident, sospita d'incident, desviació de seguretat, ús indegut d'accessos, pèrdua de control sobre informació, vulnerabilitat rellevant

o incompliment de política que pugui afectar la confidencialitat, integritat, disponibilitat o traçabilitat de la informació o dels serveis.

- Garantir que tot el personal assignat al servei rep formació, informació i conscienciació sobre les obligacions de seguretat, confidencialitat, protecció de dades, ús acceptable dels sistemes, gestió d'incidents i compliment de les polítiques corporatives, amb evidències disponibles per a l'Agència quan siguin requerides.

A la finalització del contracte, en cas de canvi de recurs o quan l'Agència ho requereixi, l'adjudicatari quedarà obligat al lliurament, retorn, eliminació segura o destrucció de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei, d'acord amb les instruccions de l'Agència. Aquesta actuació haurà d'incloure la revocació d'accessos, la retirada de credencials, la confirmació de no conservació de còpies no autoritzades i el lliurament de les evidències corresponents.

3.10 Control de Gestió

L'adjudicatari, i especialment el Coordinador del Servei, haurà de col·laborar de manera activa amb l'Àrea d'Assessoria Jurídica i Contractació i els òrgans de govern de l'Agència, amb l'objectiu de garantir un seguiment econòmic-operatiu rigorós, traçable i alineat amb els productes, lliurables, KPIs, ANS i mecanismes de governança definits en aquest plec.

Aquest control haurà de permetre a l'Agència disposar d'una visió fiable sobre la capacitat assignada, la dedicació efectiva, l'evolució de la demanda, l'estat dels compromisos, el consum de recursos, la qualitat de l'execució, els riscos, les desviacions, la facturació i la previsió d'activitat futura, facilitant la presa de decisions i la priorització de la demanda.

La priorització de la capacitat disponible haurà de respectar els criteris generals de priorització del Servei TIC definits en aquest plec, especialment davant situacions de concurrència de demanda, incidències crítiques, riscos de seguretat, indisponibilitat, desviacions rellevants o conflictes entre activitats recurrents, evolutives i de millora.

- Complir el model de seguiment econòmic, planificació de capacitat, execució d'activitats, aportació d'informació per al control de dedicacions, seguiment de demanda, gestió de riscos i compliment d'ANS que determini l'Agència.
- Ajustar-se als procediments de facturació, conformació, validació de serveis, circuits d'aprovació i mecanismes de control econòmic que determini l'Agència.
- Aportar la informació i les evidències necessàries per conformar les factures en relació amb els serveis efectivament reportats, executats, validats i acceptats per l'Agència, d'acord amb els procediments establerts.
- Exercir la gestió del contracte amb capacitats de forecast, identificant i informant necessitats de capacitat, desviacions de consum, riscos pressupostaris, increments de demanda, necessitats de reforç i possibles impactes econòmics o operatius, per facilitar el control i la presa de decisions de l'Agència.
- Realitzar el reporting en les eines, plantilles, repositoris o canals proporcionats per l'Agència, assegurant la qualitat, coherència, puntualitat, traçabilitat i verificabilitat de la informació reportada.

Per dur a terme aquest control, caldrà aportar la documentació següent:

- Fitxer mestre de persones assignades al servei, amb perfil, rol, dedicació prevista, dedicació efectiva, període d'assignació, substitucions, absències cobertes i relació amb els àmbits funcionals del Servei TIC.

- Fitxer mestre de projectes, activitats, serveis, tasques recurrents, iniciatives de millora, evolucions tecnològiques i actuacions rellevants vinculades al contracte.
- Estimació de recursos, dedicacions i capacitat necessària per projecte, activitat, servei, àmbit funcional o iniciativa, incloent desviacions respecte de la previsió inicial.
- Registre i seguiment dels riscos tècnics, econòmics, organitzatius, de capacitat, de seguretat, de disponibilitat, de coneixement i de continuïtat operativa associats al servei.
- Seguiment del consum de recursos, capacitat disponible, dedicació efectiva, càrrega de treball, backlog, demanda entrant, demanda resolta i evolució mensual de l'activitat.
- Imputació de temps, activitats, tasques, projectes, incidències, peticions, canvis, suport a comitès, documentació, automatitzacions i activitats de millora contínua.
- Assignació de tasques a persones, amb indicació del responsable, estat, prioritat, termini, dependències, evidències associades i vinculació amb tiquets, projectes, lliurables o compromisos de servei.
- Memòria d'activitat del contracte, amb visió operativa i executiva de serveis prestats, resultats, fites, desviacions, riscos, millores, lliurables, incidències rellevants i evolució dels KPIs.
- Informació de facturació, conformació de factures, justificació de serveis, evidències de prestació, validacions de l'Agència i traçabilitat entre activitat reportada, servei executat i import facturable.
- Quadres de comandament, informes mensuals, informes executius i indicadors de seguiment que permetin relacionar activitat, capacitat, qualitat, ANS, riscos, costos, demanda, millores i compliment contractual.
- Registre de desviacions, accions correctores, compromisos adquirits en comitès, responsables, terminis i estats d'execució.

L'adjudicatari haurà de proporcionar informació veraç, completa, actualitzada, contrastada i traçable, i haurà de disposar dels mecanismes necessaris per garantir la qualitat de la dada, la coherència entre fonts, la conciliació entre activitat reportada i activitat executada, i la correspondència entre dedicació, lliurables, KPIs, ANS i facturació. Sempre que sigui possible, l'adjudicatari haurà d'automatitzar la generació, consolidació i transmissió de la informació, integrant-la amb les eines corporatives que determini l'Agència.

L'Agència podrà requerir informació addicional o actualitzada fora de la planificació ordinària quan sigui necessari per al govern del servei, la gestió pressupostària, el seguiment d'incidències crítiques, l'anàlisi de riscos, la preparació de comitès, la validació de factures o la presa de decisions. L'adjudicatari haurà de donar resposta en terminis compatibles amb la criticitat i naturalesa de la petició.

L'Agència podrà dur a terme auditories, verificacions o revisions sobre la informació reportada, les evidències aportades, els mecanismes d'imputació, la qualitat de la dada, la conformació de factures, la dedicació declarada i el compliment dels compromisos del servei. L'adjudicatari haurà de participar-hi de manera activa, diligent i sense cap cost addicional per a l'Agència, aportant la documentació, registres, justificacions i plans d'acció que siguin requerits.

3.11 Govern i qualitat de la documentació

Tota la documentació, materials, procediments, manuals, guies, runbooks, scripts documentats, models d'informe, registres, evidències, actes, inventaris, bases de coneixement, materials de transferència i qualsevol altre actiu documental elaborat, actualitzat o generat en el marc de la prestació del Servei TIC serà propietat de l'Agència. L'Agència disposarà del dret d'ús, reproducció,

modificació, adaptació, actualització, reutilització i explotació interna d'aquesta documentació sense cap cost addicional i sense dependències del proveïdor. El servei haurà de garantir que disposa de totes les autoritzacions, permisos i drets necessaris per donar compliment a aquesta obligació, incloent els relatius a materials elaborats per tercers o subcontractistes.

La documentació formarà part dels lliurables i evidències del servei i haurà d'estar alineada amb els productes, lliurables i KPIs definits al punt 2.2.4, amb el model de documentació i gestió del coneixement del punt 2.2.5 i amb les obligacions de gestió del coneixement establertes al punt 3.8. Aquesta documentació haurà de permetre acreditar l'execució dels serveis, el compliment dels ANS, la qualitat de la prestació, la seguretat, la continuïtat operativa, la transferència de coneixement, la millora contínua i la reversibilitat del servei.

L'adjudicatari haurà de mantenir tota la documentació en el sistema de gestió documental, repositori corporatiu o base de coneixement que determini l'Agència. La documentació haurà d'estar organitzada, classificada, versionada, actualitzada, traçable, accessible als perfils autoritzats i identificada, com a mínim, amb responsable, estat, data d'actualització, versió, àmbit funcional, criticitat i periodicitat de revisió. L'adjudicatari haurà de mantenir un inventari documental actualitzat que permeti identificar l'estat, cobertura, vigència i qualitat dels documents rellevants del Servei TIC.

L'Agència podrà definir formats, plantilles, convencions de nom, estructura de carpetes, metadades, criteris d'enllaç entre documents i eines de suport per a la documentació tècnica. Quan s'utilitzin formats com Markdown o eines com Obsidian o equivalents, l'adjudicatari haurà de garantir que la documentació sigui portable, llegible sense eines propietàries, versionable, exportable, reutilitzable i integrable amb el repositori corporatiu.

En qualsevol cas, tota la documentació i informació generada o mantinguda en el marc del contracte haurà de romandre dins del tenant Microsoft 365 de l'Agència o en els repositoris corporatius autoritzats, especialment SharePoint, OneDrive, Teams o altres serveis aprovats. No es permetrà la creació de repositoris locals, núvols personals, sincronitzacions externes o entorns documentals paral·lels no autoritzats per l'Agència.

La documentació haurà de complir criteris mínims de qualitat documental, incloent claredat, completesa, vigència, coherència amb els procediments aprovats, traçabilitat de canvis, reutilització, absència d'ambigüitats, adequació al nivell tècnic dels destinataris i alineació amb les polítiques de seguretat i governança de l'Agència. Els documents hauran d'estar redactats de manera que permetin l'operació, suport, auditoria, revisió, manteniment, transferència i continuïtat del servei sense dependències individuals excessives.

La persona o unitat designada per l'Agència serà responsable de validar i aprovar els documents lliurats pel servei. L'Agència podrà retornar qualsevol document que no compleixi els criteris de qualitat, estructura, completesa, actualització o utilitat requerits, indicant les observacions o correccions necessàries. L'adjudicatari haurà d'esmenar els documents en el termini que determini l'Agència i, fins que no siguin validats, no es consideraran lliurables acceptats a efectes de seguiment, conformació o compliment del servei.

L'adjudicatari haurà d'actualitzar la documentació sempre que es produeixin canvis en sistemes, eines, configuracions, automatitzacions, integracions, procediments, processos ITSM, inventari, CMDB, monitorització, seguretat, backup, workplace, cloud, organització de l'equip, incidències rellevants, auditories, proves de continuïtat, canvis de recurs o evolucions tecnològiques. Aquesta actualització haurà de generar les evidències corresponents i haurà de quedar reflectida en l'inventari documental i en els mecanismes de seguiment del servei.

En cas de finalització del contracte, canvi de proveïdor, canvi de recurs o activació de processos de reversibilitat, el servei haurà de lliurar a l'Agència un estat actualitzat, complet i validable del repositori documental, incloent l'inventari de documentació, documents crítics, procediments vigents, pendents,

riscos documentals, evidències de transferència de coneixement i qualsevol element necessari per garantir la continuïtat operativa del Servei TIC.

L'incompliment recurrent de les obligacions de documentació, qualitat documental, actualització, validació, disponibilitat, transferència o reversibilitat podrà ser considerat una desviació del servei i donar lloc als mecanismes de seguiment, correcció o penalització previstos en el contracte, especialment quan afecti la seguretat, la continuïtat operativa, la substitució de recursos, la traçabilitat, el compliment dels ANS o la capacitat de l'Agència per governar el Servei TIC.

3.12 Formació, capacitació i transferència de coneixement

L'adjudicatari haurà de garantir la capacitació contínua del personal assignat al Servei TIC com a mecanisme essencial per assegurar la qualitat de la prestació, la seguretat, la continuïtat operativa, l'adaptació a l'evolució tecnològica, la correcta aplicació dels procediments de l'Agència i la reducció del risc associat a dependències individuals o manca d'actualització tècnica.

A aquest efecte, l'adjudicatari haurà de presentar, mantenir i executar un Pla anual de formació i capacitació del servei, alineat amb els perfils, activitats, eines, lliurables, KPIs, polítiques de seguretat, gestió del coneixement, qualitat documental i evolució tecnològica definits en aquest plec. Aquest pla haurà de ser validat per l'Agència i haurà d'incloure, com a mínim, objectius, perfils afectats, continguts, calendari, dedicació prevista, accions formatives, certificacions previstes quan correspongui, formació obligatòria, evidències, indicadors de seguiment i impacte esperat en la qualitat del servei.

L'adjudicatari haurà de reservar, com a mínim, un 2% anual del temps del personal assignat al servei per a tasques de formació, capacitació i certificació en matèries directament relacionades amb l'activitat del contracte. Aquest temps tindrà caràcter no facturable, no podrà comportar cap increment de cost per a l'Agència i s'haurà de planificar de manera que no redueixi la capacitat ordinària compromesa, no degradi la cobertura del servei i no afecti el compliment dels ANS.

El Pla anual de formació i capacitació haurà d'estar orientat, com a mínim, als àmbits següents: seguretat corporativa, ENS, protecció de dades, confidencialitat i ús acceptable dels sistemes; Microsoft 365, Entra ID, Intune, Defender, Azure Virtual Desktop i govern del lloc de treball digital; Azure, govern cloud, control de costos i configuració segura; ITSM, OTRS, gestió d'incidents, peticions, problemes i canvis; monitorització, observabilitat, Zabbix i capacitats d'analítica avançada; backup, recuperació, Cohesity i continuïtat operativa; inventari, CMDB i Lansweeper; automatització, scripting, runbooks i integracions; documentació, gestió del coneixement, qualitat documental i transferència de coneixement; així com les eines, procediments i metodologies específiques que determini l'Agència durant la vigència del contracte.

El Pla anual de formació i capacitació haurà d'incloure accions específiques sobre l'ús segur, responsable i productiu de les capacitats d'intel·ligència artificial autoritzades per l'Agència, especialment Microsoft 365 Copilot, Copilot Studio i Security Copilot. Aquesta formació haurà de cobrir, com a mínim, casos d'ús aprovats, bones pràctiques de prompting, limitacions de les eines, verificació de resultats, protecció de dades, classificació de la informació, riscos d'ús indegut, supervisió humana, registre d'evidències i integració amb els processos del Servei TIC.

La formació en matèria de seguretat, confidencialitat, protecció de dades, compliment normatiu, gestió d'incidents de seguretat i aplicació de les polítiques corporatives tindrà caràcter obligatori per a tot el personal assignat al servei, tant en la incorporació inicial com quan es produeixin canvis normatius, tecnològics, organitzatius o de procediment que ho facin necessari.

Quan s'incorporin noves eines, automatitzacions, procediments, integracions, plataformes, models d'accés, canvis rellevants de servei o evolucions tecnològiques, l'adjudicatari haurà de garantir la formació del seu personal i, quan l'Agència ho requereixi, la transferència de coneixement cap als

equips de l'Agència o tercers autoritzats. Aquesta transferència haurà d'anar acompanyada de materials, sessions, documentació, evidències i actualització de la base de coneixement o repositori documental corresponent.

L'adjudicatari haurà de mantenir evidències actualitzades de l'execució del pla de formació, incloent registre d'accions formatives, assistència, hores dedicades, continguts impartits, materials utilitzats, certificats o acreditacions obtingudes, resultats o avaluacions quan apliqui, i relació de les accions formatives amb necessitats del servei, millores, canvis, riscos o evolucions tecnològiques. Aquest seguiment s'haurà d'incorporar als mecanismes de reporting i control de gestió definits en aquest plec.

Les certificacions o accions formatives del personal del servei hauran d'estar relacionades amb els perfils assignats i amb les necessitats reals del Servei TIC. Qualsevol cost associat a la formació, capacitació o certificació del personal del servei serà assumit per l'adjudicatari, excepte previsió expressa en contrari, i no podrà ser repercutit a l'Agència ni afectar la prestació ordinària del servei.

El Pla anual de formació i capacitació s'haurà de coordinar amb les activitats i accions formatives pròpies de l'Agència, especialment quan afectin eines corporatives, procediments interns, polítiques de seguretat, nous serveis, canvis operatius o iniciatives de transformació tecnològica. L'incompliment recurrent de les obligacions de formació, evidència, capacitació o transferència de coneixement podrà ser considerat una desviació del servei quan afecti la qualitat, seguretat, continuïtat, documentació, compliment dels ANS o capacitat operativa del Servei TIC.

3.13 Continuïtat operativa i pla de contingència del servei

L'adjudicatari haurà de disposar d'un pla de continuïtat operativa i contingència del Servei TIC que permeti mantenir, recuperar o restablir la prestació dels serveis davant situacions d'indisponibilitat, degradació greu, desastre, ciberincident, indisponibilitat d'eines corporatives, pèrdua d'accés remot, afectació d'instal·lacions, indisponibilitat de personal crític o qualsevol altra circumstància que pugui comprometre la continuïtat del servei.

Aquest pla haurà d'incloure, com a mínim:

- Identificació d'escenaris de contingència, serveis crítics, dependències tecnològiques, dependències de personal, eines corporatives, accessos, comunicacions, plataformes cloud, entorns de treball digital i processos ITSM afectats.
- Definició de mecanismes alternatius de prestació, incloent accés segur remot, entorns corporatius controlats, canals alternatius de comunicació, redistribució de capacitat, suport expert, ús d'eines autoritzades i procediments manuals temporals quan sigui necessari.
- Priorització de serveis, activitats i funcionalitats segons criticitat, impacte en usuaris, seguretat, disponibilitat, continuïtat operativa i compliment dels ANS.
- Definició d'objectius de recuperació, temps màxims de resposta, criteris d'activació, rols, responsables, canals d'escalat i mecanismes de coordinació amb l'Agència, Seguretat Corporativa, CTTI i altres proveïdors quan correspongui.
- Execució de proves periòdiques, simulacres o validacions del pla de contingència amb la periodicitat que determini l'Agència, generant evidències, conclusions, desviacions, accions correctores i actualitzacions documentals.

El pla haurà d'estar alineat amb els ANS, els plans de continuïtat de l'Agència, el model d'accés segur definit al punt 3.7, la gestió del coneixement del punt 3.8, les obligacions de seguretat del punt 3.9 i el govern documental del punt 3.11. L'adjudicatari haurà de mantenir el pla actualitzat durant tota la vigència del contracte i revisar-lo després de qualsevol prova, incident rellevant, canvi tecnològic, canvi organitzatiu o modificació substancial del servei.

Als efectes d'aquest contracte, s'entendrà per fita de continuïtat qualsevol activitat planificada, obligació o acció identificada en el Pla de Continuïtat Operativa o en el Pla de Contingència del Servei TIC que tingui com a finalitat verificar, mantenir o millorar la capacitat de continuïtat, recuperació o resposta davant situacions de contingència.

Com a mínim, es consideraran fites de continuïtat:

- Elaboració inicial del Pla de Continuïtat Operativa.
- Revisió periòdica del pla.
- Actualització del pla després de canvis rellevants.
- Execució de proves de restauració.
- Execució de simulacres o proves de contingència.
- Validació dels procediments de recuperació.
- Revisió de dependències crítiques.
- Actualització dels inventaris i documentació de continuïtat.
- Execució de les accions correctores derivades de proves o simulacres.
- Qualsevol altra activitat de continuïtat formalment aprovada o requerida per l'Agència.

Es considerarà una fita completada quan disposi de les evidències corresponents i hagi estat validada per l'Agència. Com a evidències vàlides s'acceptaran, entre d'altres, plans aprovats, actes de revisió, informes de proves, registres ITSM, evidències tècniques, plans d'acció, registres de seguiment i actes de validació emesos per l'Agència.

L'activació del pla de contingència no suspendrà els ANS ni eximirà l'adjudicatari de les seves responsabilitats contractuals, excepte en els supòsits expressament previstos al contracte. L'adjudicatari haurà de documentar l'activació, execució, recuperació i tancament de qualsevol situació de contingència, incloent causes, impacte, decisions adoptades, temps de resposta, serveis afectats, mesures correctores i lliçons apreses.

3.14 Metodologia de treball, estàndards i gestió de lliurables

L'organització del treball, l'execució de les activitats, la gestió dels lliurables i el seguiment del Servei TIC s'hauran d'adequar a les metodologies, estàndards, procediments i eines que determini l'Agència durant la vigència del contracte. L'adjudicatari haurà d'aplicar un model de treball estructurat, traçable, documentat i orientat a resultats, alineat amb ITSM, bones pràctiques ITIL, ENS, ISO/IEC 20000, ISO/IEC 27001 o marcs equivalents quan siguin aplicables.

La metodologia haurà de garantir la traçabilitat entre requeriments, activitats, tasques, tiquets, canvis, riscos, evidències, lliurables, KPIs i ANS. Qualsevol lliurable haurà d'estar identificat, versionat, validable, associat al seu àmbit funcional, responsable, estat, data de lliurament, criteri d'acceptació i, quan correspongui, vinculació amb els productes i indicadors definits al punt 2.2.4.

Cada lliurable haurà de disposar, com a mínim, d'un responsable identificat, periodicitat o fita de lliurament, criteri d'acceptació, format esperat, font d'evidència, estat de validació i relació amb l'objectiu, activitat, producte, KPI o ANS corresponent. L'Agència podrà requerir l'esmena, actualització o ampliació de qualsevol lliurable que no sigui complet, vigent, verificable, coherent amb els requisits del plec o útil per al seguiment i govern del servei.

Quan els lliurables, informes, anàlisis, documentació, automatitzacions o agents siguin generats o assistits mitjançant eines d'intel·ligència artificial, l'adjudicatari haurà d'identificar-ho quan sigui rellevant, validar-ne el contingut mitjançant supervisió humana, conservar les evidències necessàries, evitar la incorporació d'informació no autoritzada i garantir que el resultat compleix els criteris de qualitat, seguretat, traçabilitat, verificabilitat i acceptació establerts per l'Agència.

Els lliurables tècnics i operatius hauran de poder adaptar-se als formats i estàndards documentals que determini l'Agència, incloent formats estructurats, oberts i versionables com Markdown quan sigui aplicable. Aquests formats s'hauran d'utilitzar sempre dins del tenant Microsoft 365 de l'Agència o dels repositoris corporatius autoritzats, mantenint la integració amb SharePoint, OneDrive, Teams o les eines Microsoft 365 que determini l'Agència.

L'ús d'eines com Obsidian o equivalents només serà admissible quan estigui autoritzat per l'Agència i no impliqui l'extracció d'informació, la generació de còpies fora del tenant, la pèrdua de traçabilitat, la disminució dels controls de seguretat o la creació de dependències tecnològiques.

L'adjudicatari haurà de gestionar els canvis, riscos, desviacions i dependències mitjançant procediments aprovats, evidències verificables, registre d'acords i mecanismes de validació per part de l'Agència, i haurà d'executar les decisions rellevants adoptades per l'Agència. També haurà d'adaptar-se a noves metodologies, eines o estàndards que l'Agència implanti durant el contracte, sense cost addicional i sense degradar la prestació del servei.

Als efectes d'aquest contracte, s'entendrà per element de reversibilitat qualsevol informació, documentació, coneixement, configuració, accés, inventari, automatització, lliurable o actiu necessari per permetre la continuïtat del Servei TIC en cas de transició, canvi de proveïdor, internalització del servei o finalització del contracte.

Com a mínim, es consideraran elements de reversibilitat:

- Inventari actualitzat d'actius i serveis.
- Inventari d'identitats i accessos.
- Inventari de plataformes i dependències.
- CMDB i mapes de servei.
- Procediments operatius.
- Runbooks i automatitzacions.
- Scripts i integracions.
- Documentació tècnica i funcional.
- Inventari documental.
- Base de coneixement.
- Configuracions de referència.
- Plans de continuïtat i contingència.
- Registre de riscos oberts.
- Registre d'incidències i canvis rellevants.
- Evidències de transferència de coneixement.
- Qualsevol altre element que l'Agència consideri necessari per assegurar la continuïtat operativa del servei.

Es considerarà element lliurat i validat quan disposi de l'evidència corresponent i hagi estat acceptat formalment per l'Agència.

3.15 Obligacions específiques de seguretat, confidencialitat i protecció de dades

Aquest apartat recull les obligacions específiques de caràcter normatiu, legal i contractual en matèria de seguretat de la informació, confidencialitat, protecció de dades, compliment de l'ENS, interconnexions, auditoria, incidents i accés a informació de seguretat. Aquestes obligacions

complementen, sense substituir-les, les obligacions operatives de Seguretat Corporativa establertes al punt 3.9.

3.15.1 Deure de confidencialitat

Tot el personal de l'adjudicatari, així com els possibles subcontractistes o tercers que participin en l'execució del contracte, hauran de mantenir absoluta confidencialitat i estricte secret sobre qualsevol informació oral, escrita, digital, tècnica, operativa, documental, organitzativa o de seguretat coneguda com a conseqüència de la prestació dels serveis. Aquesta informació no podrà ser utilitzada per a finalitats diferents de l'execució del contracte ni comunicada a tercers sense autorització expressa de l'Agència.

L'obligació de confidencialitat s'haurà de mantenir durant el termini previst al contracte i, en tot cas, durant un mínim de 10 anys des que es va tenir coneixement de la informació, excepte en relació amb les dades personals, respecte de les quals el deure de confidencialitat tindrà caràcter indefinit d'acord amb la normativa aplicable. L'adjudicatari haurà de comunicar aquesta obligació al seu personal, subcontractistes i tercers, controlar-ne el compliment i formalitzar els compromisos individuals que l'Agència pugui requerir.

L'adjudicatari haurà de posar en coneixement de l'Agència, de forma immediata, qualsevol incidència, accés indegut, pèrdua de control, divulgació no autoritzada o sospita que pugui afectar la confidencialitat, integritat, disponibilitat o traçabilitat de la informació. A la finalització del contracte, o quan l'Agència ho requereixi, haurà de retornar, eliminar o destruir de manera segura la informació, aportant les evidències corresponents.

3.15.2 Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'adjudicatari actuarà, quan correspongui, com a encarregat del tractament i haurà de donar compliment al Reglament General de Protecció de Dades, a la LOPDGDD, a les instruccions documentades de l'Agència i a qualsevol altra normativa aplicable. L'adjudicatari només podrà tractar les dades per a les finalitats vinculades a l'execució del contracte i d'acord amb les instruccions rebudes.

L'adjudicatari haurà d'aplicar mesures tècniques i organitzatives adequades, garantir la confidencialitat del personal autoritzat, gestionar la subcontractació d'acord amb la normativa aplicable, assistir l'Agència en l'exercici de drets, en la gestió de violacions de seguretat, en auditories i en requeriments d'autoritats competents, i retornar o suprimir les dades personals quan finalitzi la prestació, excepte obligació legal de conservació.

3.15.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'adjudicatari 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 amb el marc legal en matèria de ciberseguretat i, en concret, amb el compliment de l'Esquema Nacional de Seguretat (ENS), l'adjudicatari 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'adjudicatari el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'adjudicatari 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'adjudicatari haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat de 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'adjudicatari haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

3.15.4 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'adjudicatari 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-ne la disposició efectiva.

L'adjudicatari 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 qual tingui accés.

3.15.5 Adquisició de productes, eines 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'adjudicatari 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 poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

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

3.15.6 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes utilitzats per a la prestació del servei 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'adjudicatari 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'adjudicatari haurà de participar en els mecanismes de coordinació que estableixi l'Agència i seguir els procediments establerts per aquest fi, per tal de poder atribuir i exercir de manera efectiva les responsabilitats en relació amb cada sistema interconnectat.

3.15.7 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'adjudicatari haurà de disposar dels recursos adients per dur a terme l'execució de les tasques que li corresponguin en relació amb aquest model de compliment, donant resposta en els terminis marcats per l'Agència. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència.

3.15.8 Incidents de seguretat

El POC haurà de notificar a l'Agència 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 l'Agència o els procediments establerts. L'adjudicatari haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'Agència.

En cas que sigui necessari, l'adjudicatari haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'Agència per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

3.15.9 Accés a la informació

L'adjudicatari haurà de garantir l'accés del personal autoritzat de l'Agència a la informació de seguretat, incloent procediments, registre d'incidents, traces i altres evidències necessàries per poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per al personal autoritzat i prèviament identificat. L'Agència i l'adjudicatari establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, amb els controls de seguretat mínims que corresponguin.

3.16 Qualitat del servei i millora contínua

L'adjudicatari haurà de vetllar per la qualitat, l'estabilitat, la seguretat, l'eficiència i la millora contínua dels processos, serveis, components tècnics, lliurables i activitats sota el seu abast, assegurant l'alineació amb els objectius del Servei TIC, els ANS, els KPIs, els requisits de documentació i els mecanismes de governança definits en aquest plec.

Per garantir aquest enfocament, l'adjudicatari haurà d'elaborar, mantenir i executar un Pla de Qualitat i Millora Contínua, validat per l'Agència, que inclogui objectius, indicadors, responsables, calendari, mecanismes de seguiment, accions preventives, accions correctores, anàlisi de causes arrel, priorització de millores i evidències d'execució.

Les principals activitats de millora contínua són:

- Anàlisi de KPIs, ANS, incidències, peticions, problemes, canvis, recurrències, riscos, desviacions, qualitat documental, experiència d'usuari i dades de control de gestió.
- Identificació d'accions de millora orientades prioritàriament a seguretat, disponibilitat, continuïtat, automatització, reducció d'intervenció manual, qualitat documental, eficiència operativa i optimització de costos.
- Identificació de casos d'ús d'intel·ligència artificial, Copilot i automatització cognitiva que aportin valor mesurable al Servei TIC, prioritzant aquells que millorin la seguretat, disponibilitat, qualitat documental, resposta a incidències, eficiència operativa, reutilització del coneixement i reducció d'intervenció manual.
- Definició d'accions preventives i correctores amb responsable, termini, benefici esperat, riscos, dependències, esforç estimat, criteris d'èxit i indicadors de seguiment.
- Seguiment periòdic en els comitès de servei, amb registre d'estat, evidències, desviacions, decisions i tancament formal de les accions aprovades.
- Revisió contínua de la qualitat percebuda, del grau de satisfacció dels usuaris, de l'eficiència dels processos i de la reutilització del coneixement generat.

3.17 Seguiment, reporting i comitès del servei

L'adjudicatari haurà de garantir un model de seguiment, reporting i comitès que permeti a l'Agència donar suport al govern del Servei TIC amb informació fiable, actualitzada, traçable i orientada a la presa de decisions. Aquest apartat regula el seguiment funcional i executiu del servei, sense perjudici del control econòmic-operatiu establert al punt 3.10.

En cas de concurrència de demandes, incidències, riscos, desviacions o necessitats d'actuació que excedeixin la capacitat ordinària disponible, la priorització del Servei TIC haurà de seguir els criteris establerts per l'Agència i, amb caràcter general, l'ordre següent: seguretat, disponibilitat, continuïtat operativa, compliment normatiu, impacte en usuaris, eficiència operativa, automatització i millora contínua. Aquesta priorització haurà de quedar reflectida en els mecanismes de seguiment, reporting, comitès, backlog, plans d'acció i registres de decisió del servei.

El seguiment del servei haurà d'incloure, quan s'hagin activat capacitats d'intel·ligència artificial o Copilot, informació sobre casos d'ús en explotació, ús real, beneficis obtinguts, riscos detectats, incidències, controls aplicats, qualitat dels resultats, accions de millora, adopció per part dels usuaris autoritzats i grau d'alineació amb els objectius de seguretat, eficiència i qualitat del Servei TIC.

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

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

Qualsevol especificitat addicional en aquest àmbit es recollirà, si escau, al contracte.

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'adjudicatari haurà de donar suport a la generació i lliurament de 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 d'aquest 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'adjudicatari s'haurà de comprometre a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'adjudicatari s'haurà de comprometre 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'adjudicatari 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'adjudicatari hi donarà resposta ràpida fora de la planificació establerta.

3.18 Integració amb altres equips

L'adjudicatari 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 l'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.
- Definició d'una matriu mínima de responsabilitats operatives, preferentment en format RACI o equivalent, que identifiqui per als principals processos, serveis, lliurables, escalats i decisions

les responsabilitats de l'Agència, el Servei TIC, Seguretat Corporativa, Aprovisionament, CTTI i altres proveïdors o equips implicats.

4 Acords de nivell de servei i penalitzacions

Aquest apartat estableix el model d'Acords de Nivell de Servei (ANS), indicadors, evidències, mecanismes de seguiment i penalitzacions aplicables al Servei TIC. El model té per finalitat assegurar que les obligacions descrites en el plec esdevinguin compromisos mesurables, traçables, verificables i contractualment exigibles, alineats amb els objectius de seguretat, disponibilitat, continuïtat operativa, escalabilitat, automatització, eficiència, qualitat documental i governança definits als apartats anteriors.

L'adjudicatari resta obligat al compliment íntegre de les prestacions, activitats, funcionalitats, productes, lliurables, evidències, KPIs i ANS establerts en aquest plec, així com dels compromisos assumits en la seva oferta i de les prescripcions del contracte. L'incompliment d'aquests compromisos podrà donar lloc a l'aplicació dels mecanismes de seguiment, correcció, compensació, penalització o resolució previstos en aquest apartat, en el contracte i en la normativa contractual aplicable.

4.1 Principis generals del model d'ANS

Els ANS s'aplicaran sobre tots els àmbits funcionals del Servei TIC, incloent infraestructura, sistemes, cloud, Microsoft 365, identitat, dispositius, lloc de treball digital, accés remot segur, seguretat TIC, backup, monitorització, ITSM, inventari, CMDB, documentació, gestió del coneixement, automatització, governança, reporting, transició, reversibilitat i suport a l'evolució tecnològica. Els ANS no substitueixen la resta d'obligacions del plec, sinó que en constitueixen el mecanisme principal de mesura, seguiment i exigibilitat.

Tots els indicadors hauran d'estar suportats per evidències objectives, verificables i disponibles per a l'Agència, procedents preferentment de les eines corporatives autoritzades, com ara OTRS, Zabbix, Lansweeper, Microsoft 365, Entra ID, Intune, Defender, Azure, Cohesity, SharePoint, Teams, registres d'activitat, informes de servei, quadres de comandament, actes de comitè, inventaris, CMDB, repositoris documentals i qualsevol altra font aprovada per l'Agència.

A efectes del càlcul del compliment global dels ANS, s'entén per **ANS aplicables** el conjunt de codis ANS del catàleg vigent que, durant el període d'avaluació, disposen d'abast efectiu, activitat mesurable, font de dada disponible i evidència suficient per ser avaluats. No es consideraran aplicables els ANS que, en aquell període, no tinguin activitat associada, no corresponguin a serveis o funcionalitats activades, estiguin subjectes a exclusió justificada o depenguin d'una fita encara no exigible. S'entén per **ANS complerts** el nombre d'ANS aplicables que, un cop mesurats i validats amb les evidències corresponents, assoleixen el llindar exigit per al període d'avaluació sense desviació penalitzable.

4.2 Matriu de priorització, impacte i temps de resolució

La classificació, priorització, escalat i seguiment de les incidències, peticions, problemes i consultes gestionades pel Servei TIC es realitzarà mitjançant una matriu comuna de priorització basada en els criteris d'impacte, urgència, criticitat, afectació a la seguretat, afectació a la disponibilitat dels serveis i impacte sobre els usuaris. Aquesta matriu constitueix la referència contractual per determinar els terminis aplicables als ANS relacionats amb la gestió ITSM, especialment els codis STICITSM01, STICITSM02, STICITSM03 i STICITSM04. La prioritat assignada haurà de quedar registrada a l'eina ITSM corporativa juntament amb la justificació corresponent. Qualsevol canvi de prioritat, reclassificació o excepció haurà de quedar degudament documentat i traçable. L'Agència es reserva la facultat de validar, modificar o reclassificar la prioritat assignada quan consideri que aquesta no s'ajusta a l'impacte real, al risc associat o als criteris establerts en aquest plec.

Criteris generals de priorització

- Impacte sobre serveis crítics de l'Agència.
- Nombre d'usuaris afectats.
- Impacte sobre la seguretat de la informació.
- Impacte sobre la disponibilitat dels serveis.
- Impacte sobre la continuïtat operativa.
- Compliment normatiu o regulatori.
- Existència o no d'alternatives operatives temporals.
- Risc de degradació o propagació de l'afectació.

Matriu de priorització

Prioritat	Descripció
P1 - Crítica	Afectació crítica a la disponibilitat, seguretat o continuïtat operativa d'un servei essencial. No existeix alternativa operativa viable.
P2 - Alta	Afectació rellevant a un servei important, amb impacte significatiu sobre usuaris o processos, però amb possibilitat de mitigació temporal.
P3 - Mitjana	Afectació limitada, amb impacte reduït o controlable i amb alternatives operatives disponibles.
P4 - Baixa	Consultes, peticions estàndard, incidències menors o actuacions sense impacte rellevant en la prestació dels serveis.

Temps objectiu per a incidències (STICITSM01)

Prioritat	Temps màxim de resposta	Temps objectiu de resolució
P1	30 minuts	4 hores
P2	1 hora	8 hores laborables
P3	4 hores laborables	3 dies laborables
P4	1 dia laborable	5 dies laborables

Temps objectiu per a peticions de servei (STICITSM02)

Prioritat	Temps màxim de resposta	Temps objectiu de resolució
P1	1 hora	1 dia laborable
P2	4 hores laborables	3 dies laborables
P3	1 dia laborable	5 dies laborables
P4	2 dies laborables	10 dies laborables

Temps objectiu per a problemes (STICITSM03)

Prioritat	Temps màxim d'inici d'anàlisi	Temps màxim de presentació de pla d'acció

P1	1 dia laborable	5 dies laborables
P2	2 dies laborables	10 dies laborables
P3	5 dies laborables	20 dies laborables

Els problemes es gestionaran mitjançant anàlisi de causa arrel i pla d'acció associat.

Temps objectiu per a consultes (STICITSM04)

Prioritat	Temps màxim de resposta
P1	4 hores laborables
P2	1 dia laborable
P3	3 dies laborables
P4	5 dies laborables

Regles de mesura

Els temps es calcularan a partir dels registres de l'eina ITSM corporativa o del mecanisme que determini l'Agència. Quan una actuació requereixi la intervenció de fabricants, tercers, CTTI o altres proveïdors externs, el servei mantindrà la responsabilitat de seguiment, coordinació, comunicació i escalat, sense perjudici de les exclusions justificades definides en aquest plec. Qualsevol excepció, suspensió de còmput, reclassificació de prioritat o causa de no aplicació haurà de quedar registrada, justificada i validada per l'Agència.

Període inicial d'estabilització

Durant els tres primers mesos de prestació del servei, l'Agència podrà revisar els llindars, terminis i criteris de classificació definits en aquesta matriu a partir de les dades reals observades durant la fase de transició i estabilització del servei. Aquesta revisió tindrà per objectiu ajustar el model a la volumetria, criticitat, dependències i comportament operatiu real del Servei TIC, sense perjudici de l'obligació del servei de prestar el servei amb diligència, traçabilitat, seguretat i continuïtat des de l'inici de la prestació.

4.3 Catàleg d'ANS del Servei TIC

Àmbit	Codi	Indicador	Descripció i fórmula	Periodicitat	Llindar inicial	Llindar final	Penalització màxima
Governança	STICGOV01	Compliment global dels ANS	Percentatge de compliment satisfactori d'ANS del catàleg. $$Càlcul = \left(\frac{\#\ d'ANS\ complerts}{\#\ d'ANS\ aplicables}\right) x\ 100$$	Mensual	95%	85%	5% del cost mensual del servei.
ITSM	STICITSM01	Resolució d'incidències en termini	*Percentatge d'incidències resoltes dins del termini acordat segons prioritat i impacte.* $$Càlcul = \left(\frac{\#\ incidències\ resoltes\ en\ termini}{\#\ incidències\ resoltes}\right) x\ 100$$	Mensual	90%	80%	5% del cost mensual del servei.
ITSM	STICITSM02	Resolució de peticions en termini	Percentatge de peticions resoltes dins del termini acordat. $$Càlcul = \left(\frac{\#\ peticions\ resoltes\ en\ termini}{\#\ peticions\ resoltes}\right) x\ 100$$	Mensual	90%	80%	5% del cost mensual del servei.
ITSM	STICITSM03	Resolució de problemes en termini	Percentatge de problemes resolts dins del termini acordat. $$Càlcul = \left(\frac{\#\ problemes\ resolts\ en\ termini}{\#\ problemes\ resolts}\right) x\ 100$$	Mensual	90%	80%	5% del cost mensual del servei.
ITSM	STICITSM04	Resolució de consultes en termini	Percentatge de consultes resoltes dins del termini acordat. $$Càlcul = \left(\frac{\#\ consultes\ resoltes\ en\ termini}{\#\ consultes\ resoltes}\right) x\ 100$$	Mensual	90%	80%	5% del cost mensual del servei.

Disponibilitat	STICDISP01	Disponibilitat dels serveis crítics gestionats	Percentatge de disponibilitat dels serveis crítics sota l'abast del Servei TIC, excloent les finestres de manteniment aprovades per l'Agència i les causes justificades no imputables a l'adjudicatari. $Càlcul = \left(\frac{temps\ de\ disponibilitat\ dels\ serveis\ crítics}{temps\ total\ del\ període}\right) x\ 100$	Mensual	99%	97%	10% del cost mensual del servei.
Monitorització	STICOBS01	Alertes crítiques amb diagnòstic documentat	Percentatge d'alertes crítiques amb diagnòstic, acció o escalat documentat. $Càlcul = \left(\frac{\#\ alertes\ crítiques\ tractades}{\#\ alertes\ crítiques\ rebudes}\right) x\ 100$	Mensual	95%	85%	5% del cost mensual del servei.
Backup	STICBCK01	Execució correcta de còpies de seguretat	Percentatge de còpies de seguretat executades correctament sobre actius coberts per política. $Càlcul = \left(\frac{\#\ còpies\ de\ seguretat\ executades\ correctament}{\#\ còpies\ de\ seguretat\ executades}\right) x\ 100$	Mensual	98%	95%	10% del cost mensual del servei.
Backup	STICBCK02	Proves de restauració satisfactòries	Percentatge de proves de restauració complertes*. *Es considerarà complerta una prova de restauració únicament quan hagi estat executada íntegrament d'acord amb el procediment aprovat, hagi obtingut un resultat satisfactori i disposi d'evidència documental validada. Les proves fallides, incompletes o sense evidència no computaran com a proves satisfactòries. Aquesta mètrica es calcularà sobre el total de proves planificades per al període objecte de mesura. $Càlcul = \left(\frac{\#\ còpies\ de\ restauració\ complertes}{\#\ còpies\ de\ restauració\ planificades}\right) x\ 100$	Trimestral	95%	85%	5% del cost mensual del servei.

Identitat i dispositius	STICIDM01	Dispositius conformes	Percentatge de dispositius gestionats* en estat de compliance "Compliant**" amb les polítiques corporatives aplicables. *S'entén per dispositiu gestionat tot aquell dispositiu enrolat al MDM de l'Agència durant almenys 14 dies **El dispositiu compleix totes les polítiques corporatives que li son aplicables i així queda reflectit al MDM $$Càlcul = \left(\frac{\#\ dispositius\ gestionats\ en\ compliance}{\#\ dispositius\ gestionats}\right) x\ 100$$	Mensual	95%	85%	5% del cost mensual del servei.
Seguretat	STICSEC01	Remediació de desviacions crítiques de seguretat	Percentatge de desviacions crítiques de seguretat* tractades dins del termini acordat amb l'Agència o Seguretat Corporativa. *Es considerarà desviació crítica de seguretat qualsevol desviació classificada formalment com a crítica per Seguretat Corporativa de l'Agència i comunicada a l'adjudicatari mitjançant els canals corporatius establerts. Només computaran les desviacions notificades durant el període objecte de mesura. Es considerarà desviació tractada quan: - La remediació s'hagi implantat dins del termini acordat - Existeixi evidència documental suficient - Hagi estat validada per l'Agència o per Seguretat Corporativa. $$Càlcul = \left(\frac{\#\ desviacions\ crítiques\ de\ seguretat\ tractades}{\#\ desviacions\ crítiques\ de\ seguretat\ notificades}\right) x\ 100$$	Mensual	95%	85%	10% del cost mensual del servei.
Cloud i Microsoft 365	STICCLOUD01	Governança de recursos cloud	Percentatge de recursos cloud governats* del total de recursos cloud gestionats. *Es considerarà recurs cloud governat, qualsevol recurs cloud gestionat que disposi, com a mínim, de la classificació requerida, l'etiquetatge obligatori, la identificació d'un Owner i la documentació de la seva finalitat, d'acord amb les directrius de l'Agència. Els	Mensual	95%	85%	5% del cost mensual del servei.

			recursos que no compleixin qualsevol d'aquests requeriments, es consideraran no conformes. $$Càlcul = \left(\frac{\#\ recursos\ cloud\ governats}{\#\ recursos\ cloud\ gestionats}\right) x\ 100$$				
Inventari i CMDB	STICCMDB01	Qualitat de la dada d'inventari	Percentatge d'actius o elements de configuració (CI) conformes*. *Es considerarà conforme qualsevol actiu o CI gestionat que disposi de totes les dades mínimes requerides, es mantingui actualitzat d'acord amb els criteris establerts i presenti coherència amb les fonts autoritzades de referència. Qualsevol registre amb camps obligatoris incomplets, dades obsoletes o discrepàncies no justificades respecte de les fonts autoritzades es considerarà no conforme. $$Càlcul = \left(\frac{\#\ actius\ o\ CIs\ conformes}{\#\ actius\ o\ CIs\ gestionats}\right) x\ 100$$	Mensual	95%	85%	5% del cost mensual del servei.
Documentació	STICDOC01	Documentació crítica conforme	Percentatge de documentació crítica* conforme** dins del període establert. * Tipus de documentació definit al punt 3.8 del Plec ** Es considerarà conforme qualsevol document crític que disposi d'una versió vigent, hagi estat revisat dins del període establert, tingui un responsable identificat i sigui accessible i validable conforme als procediments de l'Agència. Els documents que no compleixin qualsevol d'aquests requisits es consideraran no conformes. *Els documents que no compleixin qualsevol d'aquests requisits es consideraran no conformes.* $$Càlcul = \left(\frac{\#\ documents\ crítics\ conformes}{\#\ documents\ crítics\ aplicables}\right) x\ 100$$	Mensual	95%	80%	5% del cost mensual del servei.

Reporting	STICREP01	Lliurament i qualitat de l'informe mensual	Percentatge de compliment del lliurament puntual, complet i sense errors materials de l'informe mensual de servei, incloent ANS, KPIs, riscos, incidències, millores i evidències. *Càlcul = informes mensuals lliurats puntualment, complets i sense errors materials / informes mensuals aplicables x 100.* $$Càlcul = \left(\frac{\#\ informes\ mensuals\ conformes}{\#\ informes\ mensuals}\right) x\ 100$$	Mensual	100%	67%	5% del cost mensual del servei.
Personal	STICPER01	Rotació no planificada de personal crític	Nombre de baixes o substitucions no planificades que afecten perfils crítics* sense pla de traspàs validat i sense cobertura funcional equivalent. *Perfils definits al punt 3.6 $$Càlcul = \left(\frac{\#\ rotacions\ de\ personal\ crític\ no\ conformes}{\#\ rotacions\ de\ personal\ crític\ dins\ el\ període}\right) x\ 100$$	Mensual	0	2	5% del cost mensual del servei.
Automatització	STICAUT01	Automatitzacions documentades i operatives i amb benefici verificable	Nombre mínim d'automatitzacions conformes* *Es considerarà automatització conforme qualsevol automatització, integració o runbook que: • Hagi estat aprovat per l'Agència. • Estigui documentat. • Disposi de control de versions. • Es trobi operatiu. • Disposi d'evidència de benefici operatiu. $$Càlcul = \#\ automatitzacions\ conformes\ durant\ el\ període$$	Trimestral	4	0	5% del cost anual associat al servei.

IA i Copilot	STICIA01	Governança de casos d'ús d'IA	Percentatge de casos d'ús d'IA o Copilot en explotació amb fitxa aprovada, controls de seguretat, privacitat, supervisió humana, evidències i mesura de benefici. Aquest ANS només serà aplicable quan l'Agència hagi autoritzat l'ús de capacitats d'intel·ligència artificial, disposi de les llicències o serveis necessaris i existeixin casos d'ús aprovats o en fase de validació formal. Als efectes d'aquest ANS, s'aplicarà la definició de cas d'ús d'IA o Copilot establerta al punt 2.2.3. *Càlcul = casos d'ús d'IA o Copilot en explotació amb governança completa / casos d'ús d'IA o Copilot en explotació aplicables x 100.* $Càlcul = \left(\frac{\#\ casos\ d'ús\ en\ explotació\ amb\ governança\ completa}{\#\ casos\ d'ús\ en\ en\ explotació\ aplicables}\right) x\ 100$	Trimestral	100%	80%	5% del cost mensual del servei.
Continuïtat	STICCONT01	Pla de continuïtat i contingència actualitzat	Percentatge de fites de continuïtat completades, evidenciades i validades durant el període. Aquest ANS mesura el grau de compliment de les activitats de continuïtat definides al Pla de Continuïtat Operativa del Servei TIC. Als efectes d'aquest ANS, s'aplicarà la definició de fita de continuïtat establerta al punt 3.13. $Càlcul = \left(\frac{\#\ fites\ de\ continuïtat\ completades,\ evidenciades\ i\ validades}{\#\ fites\ de\ continuïtat\ aplicables}\right) x$	Semestral	100%	0%	5% del cost mensual del servei.
Transició	STICREV01	Reversibilitat i traspàs de coneixement	Percentatge de documentació, inventari, accessos, lliurables, procediments i coneixement crític lliurat i validat en processos de transició o reversibilitat*. Aquest ANS només serà aplicable durant processos de transició, transformació, canvi de proveïdor, internalització del servei o execució del pla de reversibilitat formalment activat per l'Agència.	Segons fita	100%	80%	10% del cost mensual del servei o de la fita afectada.

			*Als efectes d'aquest ANS, s'aplicarà la definició d'element de reversibilitat establerta al punt 3.14. $Càlcul = \left(\frac{\#\ elements\ de\ reversibilitat\ lliurats\ i\ validats}{\#\ elements\ de\ reversibilitat\ aplicables}\right) x\ 100$				

4.4 Fonts de mesura i evidències

La mesura dels ANS haurà de basar-se en fonts de dada objectives, traçables i auditables. L'adjudicatari haurà de garantir la coherència entre les dades reportades, les evidències disponibles i la realitat operativa del servei. Quan hi hagi divergències entre fonts, prevaldrà la font corporativa designada per l'Agència o, si escau, el resultat de la verificació o auditoria que aquesta determini.

L'adjudicatari haurà d'aportar, com a mínim, informes de servei, extraccions de les eines corporatives, registres de tiquets, evidències de monitorització, registres d'activitat, inventaris, actes de comitè, plans d'acció, evidències documentals, registres de validació i qualsevol altra informació que permeti acreditar el compliment o incompliment dels ANS. La manca d'evidència suficient podrà ser considerada com a incompliment quan impedeixi validar el nivell de servei assolit.

Per garantir una mesura objectiva, repetible i auditable dels ANS, cada indicador haurà de tenir identificada una font autoritativa, un responsable de validació, una evidència mínima i una naturalesa d'indicador. En cas de discrepància entre fonts, prevaldrà la font autoritativa definida per l'Agència o, si escau, el criteri de validació establert pel responsable designat. La manca d'evidència mínima suficient podrà impedir la consideració de l'ANS com a complert quan aquesta mancança sigui atribuïble a l'adjudicatari.

Codi ANS	Font autoritativa	Òrgan o responsable de validació de l'Agència	Evidència mínima	Tipus d'indicador
STICGOV01	Informe mensual validat i quadre de comandament d'ANS.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Informe d'ANS, acta de comitè i registre de desviacions.	Percentual mensual.
STICITSM01	OTRS o eina ITSM corporativa.	Cap d'Unitat de Govern TIC.	Extracció de tiquets, prioritats, dates, estat i tancament.	Percentual mensual.
STICITSM02	OTRS o eina ITSM corporativa.	Cap d'Unitat de Govern TIC.	Extracció de peticions, terminis, estat i tancament.	Percentual mensual.
STICDISP01	Zabbix, Azure Monitor o eina de monitorització aprovada.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Informe de disponibilitat, finestres aprovades i incidències associades.	Percentual mensual.

STICOBS01	Zabbix, Azure Monitor, registre d'alertes i ITSM.	Cap d'Unitat de Govern TIC.	Alertes crítiques, diagnòstic, acció, escalat o tiquet associat.	Percentual mensual.
STICBCK01	Cohesity, Azure Backup o eina corporativa de backup.	Cap d'Unitat de Govern TIC.	Informe d'execució de còpies, errors, excepcions i accions correctores.	Percentual mensual.
STICBCK02	Cohesity, Azure Backup o eina corporativa de backup.	Cap d'Unitat de Govern TIC.	Acta o informe de prova de restauració amb resultat i evidència.	Percentual trimestral.
STICIDM01	Intune, Entra ID i Microsoft 365.	Cap d'Unitat de Govern TIC / Seguretat Corporativa.	Informe de compliment de dispositius i polítiques aplicades.	Percentual mensual.
STICSEC01	Defender, CrowdStrike, Palo Alto, Prisma o eina aprovada.	Seguretat Corporativa / Cap d'Unitat de Govern TIC.	Registre de desviacions crítiques, data, tractament i evidència de remediació.	Percentual mensual.
STICCLOUD01	Azure, Microsoft 365, Entra ID o quadre de govern cloud.	Cap d'Unitat de Govern TIC.	Informe de recursos, etiquetatge, responsable, finalitat i desviacions.	Percentual mensual.
STICCMDB01	Lansweeper, CMDB o eina d'inventari aprovada.	Cap d'Unitat de Govern TIC.	Informe de qualitat de dades, conciliació, actius i CIs.	Percentual mensual.
STICDOC01	SharePoint, Teams o repositori documental corporatiu.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Inventari documental, versions, responsables, dates i validació.	Percentual mensual.
STICREP01	Informe mensual de servei i actes de comitè.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Informe lliurat, registre d'acceptació, observacions i esmenes.	Binari o percentual mensual.
STICPER01	Fitxer mestre de personal i registre de canvis.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Registre de rotació, pla de traspàs, validació i cobertura.	Quantitatiu mensual.
STICAUT01	Repositori d'automatitzacions, runbooks i actes de validació.	Cap d'Unitat de Govern TIC.	Automatització aprovada, documentada, versionada, provada i operativa.	Quantitatiu anual.
STICIA01	Registre de casos d'ús d'IA i Copilot.	Cap d'Unitat de Govern TIC / Seguretat Corporativa.	Fitxa aprovada, controls, evidències d'ús, benefici i supervisió humana.	Percentual trimestral.
STICCONT01	Pla de continuïtat, proves i actes de validació.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Pla actualitzat, prova o validació, desviacions i accions correctores.	Binari semestral.
STICREV01	Pla de reversibilitat, inventari i acta de traspàs.	Cap d'Unitat de Govern TIC / Comitè de Seguiment.	Documentació lliurada, inventari, accessos, coneixement i validació.	Fita / percentual.

4.5 Càlcul de les penalitzacions

Les penalitzacions s'aplicaran quan el valor obtingut per un ANS se situï per sota o per sobre dels llindars establerts, segons la naturalesa de l'indicador. El llindar inicial (Li) és el valor a partir del qual es comença a penalitzar. El llindar final (Lf) és el valor a partir del qual s'aplica la penalització màxima (Pmax). En els indicadors en què el valor desitjable sigui superior, la penalització s'incrementarà a mesura que el valor disminueixi. En els indicadors en què el valor desitjable sigui inferior, la penalització s'incrementarà a mesura que el valor augmenti.

Amb caràcter general, i excepte que el contracte estableixi un càlcul específic, la penalització serà proporcional entre Li i Lf. Si el valor compleix o supera el llindar acceptable, la penalització serà zero. Si el valor arriba o supera el llindar final d'incompliment, s'aplicarà la penalització màxima. Quan l'ANS tingui valor binari o no disposi de llindars quantitatius, s'aplicarà la penalització indicada a la taula en funció de l'incompliment acreditat.

4.6 Aplicació, acumulació i límits

Les penalitzacions podran aplicar-se de manera individual o acumulada quan un mateix fet generi impactes diferenciats sobre diversos ANS, obligacions contractuals o àmbits del servei. No obstant això, l'Agència vetllarà perquè l'aplicació sigui proporcionada, motivada, traçable i vinculada a incompliments acreditats. L'aplicació d'una penalització no eximirà l'adjudicatari de corregir la desviació, executar plans d'acció, aportar evidències de remediació i garantir la continuïtat, seguretat i qualitat del Servei TIC.

L'import total de penalitzacions aplicables en un període no podrà superar els límits que estableixi el contracte o la normativa aplicable. En absència d'un límit específic, l'Agència podrà modular l'aplicació de les penalitzacions atenent la gravetat, recurrència, impacte, risc generat, col·laboració de l'adjudicatari, existència de causes justificades i eficàcia de les mesures correctores.

Les penalitzacions derivades de l'incompliment dels ANS tindran caràcter acumulable quan correspongui, però la seva aplicació haurà de respectar en tot cas els límits, condicions i garanties establerts al PCAP, al contracte i a la normativa de contractació pública aplicable. Aquesta acumulació no alterarà els límits màxims de penalització establerts en la documentació contractual ni els efectes que puguin derivar-se d'incompliments greus, reiterats o essencials d'acord amb el règim contractual corresponent.

4.7 Exclusions i causes justificades

Com a regla general, no s'aplicaran penalitzacions quan l'incompliment derivi de causes alienes a l'adjudicatari degudament acreditades, aturades programades aprovades per l'Agència, decisions expresses de l'Agència, indisponibilitat de serveis o plataformes fora de l'abast de responsabilitat de l'adjudicatari, força major o situacions extraordinàries que desvirtuïn la mesura. L'adjudicatari haurà de comunicar aquestes circumstàncies de manera immediata, aportar evidències suficients i proposar mesures de mitigació.

L'existència d'una causa justificada no suspèn automàticament els ANS. L'Agència valorarà cada cas atenent l'impacte, l'abast, la durada, la diligència de l'adjudicatari, les mesures alternatives activades, la qualitat de la comunicació i la traçabilitat de les evidències aportades.

4.8 Incidències en la mesura i manca de col·laboració

Quan existeixin errors materials, dades incompletes, manca d'evidències, inconsistències entre fonts o manca de col·laboració de l'adjudicatari per determinar el valor correcte d'un indicador, l'Agència

podrà considerar que l'indicador no ha assolit el nivell mínim de servei, sempre que aquesta situació sigui atribuïble a l'adjudicatari i impedeixi una validació objectiva del compliment.

Es considerarà manca de col·laboració quan l'Agència sol·liciti informació, evidències, registres o aclariments en un termini raonable i l'adjudicatari no els aporti dins del termini establert, no pugui acreditar-ne la disponibilitat o no justifiqui adequadament el retard. Aquesta situació podrà donar lloc a l'aplicació de penalitzacions, sense perjudici de les accions correctores que corresponguin.

4.9 Facturació i compensació de penalitzacions

L'import corresponent a les penalitzacions aplicades es podrà compensar en la factura del període corresponent o en la factura immediatament posterior, d'acord amb el procediment de conformació, validació i facturació que determini l'Agència. La no incorporació d'una reducció per qualsevol causa administrativa, tècnica o de tramitació no eximirà l'adjudicatari de l'obligació de satisfer l'import que correspongui.

L'Agència podrà optar, quan sigui contractualment admissible i així ho consideri convenient, per exigir compensacions en serveis equivalents, reforços temporals, plans d'acció, mesures correctores o altres mecanismes de restitució operativa, sense perjudici de la penalització econòmica que pugui correspondre.

4.10 Incompliments de seguretat, confidencialitat i normativa interna

L'incompliment de les obligacions de seguretat corporativa, confidencialitat, protecció de dades, ENS, ús d'eines, accés a informació, traçabilitat, tractament documental, ús d'intel·ligència artificial o normativa interna de l'Agència podrà ser considerat incompliment greu o molt greu, atenent la naturalesa dels fets, l'impacte potencial o real, el risc generat, la recurrència, la intencionalitat, la manca de diligència i la col·laboració de l'adjudicatari en la contenció i remediació.

En aquests supòsits, l'Agència podrà aplicar una penalització d'entre el 5% i el 15% del cost mensual del servei, sense perjudici dels límits màxims acumulats establerts al PCAP i al contracte i de la reclamació dels danys i perjudicis efectivament causats, de l'exigència de plans d'acció immediats, de la revocació d'accessos, de la substitució de recursos, de l'activació dels mecanismes de seguretat corresponents o de la facultat resolutòria prevista al contracte i a la LCSP.

L'òrgan o responsable que determini l'Agència, incloent Seguretat Corporativa quan l'incompliment afecti la seguretat de la informació, podrà iniciar el procediment de verificació, requerir informació, donar audiència a l'adjudicatari, valorar les evidències i proposar l'aplicació de la penalització o de les mesures contractuals que corresponguin.

4.11 Relació amb la LCSP i efectes contractuals

La imposició de penalitzacions i la facultat resolutòria de l'Agència per incompliment es regiran pel que estableixen els articles 192 i següents de la LCSP, pel contracte i per la resta de normativa aplicable. Les penalitzacions no tindran finalitat recaptatòria i la seva aplicació no substituirà ni minorarà la indemnització que, si escau, pugui correspondre pels danys i perjudicis derivats dels incompliments.

La reiteració d'incompliments, la manca de correcció de desviacions, la manca de col·laboració, l'afectació greu a la seguretat, la disponibilitat, la continuïtat operativa o la qualitat del Servei TIC, o l'incompliment sostingut dels ANS podrà ser considerat causa d'adopció de mesures contractuals addicionals, incloent plans d'acció obligatoris, revisió del model de servei, substitució de recursos, reforç de governança, compensacions, penalitzacions acumulades o resolució contractual, d'acord amb el marc jurídic aplicable.

5 Fases de la prestació

L'adjudicatari haurà de presentar dins la seva oferta tècnica el pla d'actuació detallat per tal de garantir les següents fases, si s'escau atenent a la situació actual de l'Agència:

5.1 Inici de la prestació

És el període comprès entre l'entrada en vigor del contracte i l'estabilització efectiva del servei en els nivells de qualitat, disponibilitat i compliment dels ANS establerts en aquest plec. **Aquesta fase tindrà una durada màxima de tres setmanes des de la formalització de l'adjudicació**, sense perjudici que determinades actuacions de consolidació documental o transferència de coneixement puguin continuar de manera puntual durant les primeres setmanes de la fase ordinària de prestació.

Durant aquesta fase, l'adjudicatari haurà d'adquirir el coneixement necessari per assumir la prestació del Servei TIC amb garanties de continuïtat, seguretat, qualitat i eficiència operativa. Amb aquesta finalitat, haurà de dur a terme les activitats de transferència de coneixement, revisió documental, anàlisi de l'entorn tecnològic, revisió dels procediments operatius, identificació de dependències, validació dels inventaris i eines de gestió, així com l'anàlisi de l'estat dels serveis, plataformes, infraestructures, sistemes, eines de seguretat, processos ITSM, mecanismes de monitorització i entorns de lloc de treball inclosos dins l'abast contractual.

L'adjudicatari haurà de coordinar-se amb l'Agència, els possibles proveïdors sortints i la resta d'agents implicats per comprendre el model de funcionament existent, els circuits operatius, els procediments d'escalat, els mecanismes de governança, els riscos coneguts, les limitacions operatives, els compromisos pendents i qualsevol altra informació necessària per garantir una assumpció ordenada i sense afectacions al servei.

Com a resultat d'aquesta fase, l'adjudicatari haurà d'elaborar i presentar a l'Agència un informe d'assumpció del servei que inclogui, com a mínim, la situació inicial identificada, les desviacions detectades, els riscos rellevants, les dependències existents, les necessitats de millora prioritzades, les accions de mitigació proposades i el pla de treball inicial per a la fase ordinària de prestació.

L'inici de la prestació haurà de desenvolupar-se sense interrupció dels serveis existents i sense impacte negatiu sobre els usuaris, els sistemes, la seguretat, la disponibilitat de les plataformes o el compliment dels Acords de Nivell de Servei vigents. L'adjudicatari serà responsable d'organitzar els recursos, mecanismes de coordinació i activitats de transició necessàries per garantir una assumpció progressiva, controlada i traçable del servei.

5.2 Prestació

Es considera la fase ordinària de prestació del servei i comprèn el període que transcorre des de la finalització de la fase d'inici de la prestació fins als quinze dies naturals anteriors a la finalització del contracte, moment en què s'iniciarà la fase de devolució. Durant aquest període, l'adjudicatari haurà d'assumir la prestació completa del Servei TIC i garantir-ne la correcta execució d'acord amb les condicions, requeriments i objectius establerts en aquest plec.

Durant aquesta fase, l'adjudicatari haurà de garantir la disponibilitat i continuïtat dels serveis sota el seu àmbit d'actuació, el compliment dels Acords de Nivell de Servei (ANS), l'aplicació de les mesures de seguretat i compliment normatiu establertes per l'Agència, així com el manteniment actualitzat de la documentació, els procediments, els inventaris i la resta d'evidències necessàries per al seguiment i govern del servei.

L'adjudicatari haurà de mantenir una actitud proactiva orientada a la identificació de riscos, dependències, obsolescències, incidències recurrents i oportunitats de millora, proposant les actuacions que contribueixin a incrementar la qualitat, la seguretat, l'eficiència operativa, l'automatització i l'evolució tecnològica dels serveis, sempre sota les directrius i criteris de priorització establerts per l'Agència.

Durant tota la vigència d'aquesta fase s'aplicaran els mecanismes de seguiment i millora contínua del servei. Com a mínim amb periodicitat mensual, es revisarà l'estat dels serveis, el compliment dels ANS, els riscos, les desviacions identificades i les accions de millora en els corresponents òrgans de seguiment, amb l'objectiu de garantir l'alineament permanent del servei amb les necessitats de l'Agència i la seva evolució tecnològica i organitzativa.

5.3 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la cancel·lació del contracte, i que comença **quinze dies** abans de l'extinció d'aquest. Durant aquesta fase hi haurà coexistència amb un nou adjudicatari fins que es transfereixin els serveis a aquest.

L'adjudicatari haurà de procurar la metodologia, eines i recursos necessaris per tal de traspassar adequadament el servei a altres possibles futurs adjudicataris.

Tot el material generat i desenvolupat és propietat de l'Agència i romandrà, amb tota la seva documentació, a l'Agència un cop acabada la prestació del servei.

Tal i com s'ha descrit a l'apartat **3.7 Eines i equipament per a la prestació de serveis**, els mitjans tècnics que el proveïdor sortint hagi proporcionat per tal de desenvolupar la seva tasca hauran de ser degudament esborrats i tota la informació traspassada a qui l'Agència designi.

La retirada, retorn, revocació d'accessos, eliminació segura de la informació i cessament d'ús de les eines, equips i recursos emprats durant la prestació del servei es regiran segons l'establert a l'apartat **3.7 Eines i equipament per a la prestació de serveis** i a la resta de condicions de reversibilitat definides en aquest plec.