PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE PRESTACIÓ DELS SERVEIS DE MANTENIMENT I ADMINISTRACIÓ DE LES INFRASTRUCTURES TIC DEL CENTRE DE PROCESSOS DE DADES DEL CONSORCI INSTITUT RAMON LLULL

Expedient G0935 N-331/25 | Manteniment infraestructures TIC (CPD)

Taula de continguts

1 OBJECTE DEL CONTRACTE

L'objecte d'aquest plec és establir les prescripcions tècniques que han de regir la contractació dels serveis TIC del Centre de Processament de Dades (CPD) del Consorci Institut Ramon Llull (en endavant, l'Institut o el Consorci), amb l'objectiu de garantir la continuïtat operativa del CPD durant el període de transició fins a la seva migració completa als serveis CLOUD del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI), prevista per a finals de 2026.

Aquesta contractació inclou el servei d'administració i gestió tècnica del CPD, i el manteniment integral de sistemes. Aquest últim inclou el manteniment correctiu i preventiu del maquinari (hardware), el servei de còpies de seguretat remotes, el servei de *Disaster Recovery* amb capacitat de restauració en 48 hores i el manteniment del sistema d'alimentació ininterrompuda (SAI).

Al capítol 4 es detallen els objectius i funcions de cadascun d'aquests serveis a què ha de donar resposta l'empresa adjudicatària.

2 NECESSITAT I IDONEÏTAT DEL CONTRACTE

L'Institut és una entitat de dret públic de caràcter associatiu, dotada de personalitat jurídica pròpia i sense ànim de lucre, integrada per l'Administració de la Generalitat de Catalunya, l'Administració de la comunitat autònoma de les Illes Balears, l'Ajuntament de Barcelona i l'Ajuntament de Palma. La seva missió és la projecció i difusió internacional de la llengua i la cultura catalanes en totes les seves expressions. En aquest marc, l'Institut dona suport a les polítiques de relacions exteriors en l'àmbit cultural de les institucions consorciades.

Per al compliment dels seus objectius, l'Institut compta amb una plantilla prevista per a l'any 2025 de 86 persones treballadores, principalment a la seu de Barcelona, així com personal destinat a l'exterior i participants al programa de residències Faber. Per garantir la correcta operativa dels diferents perfils d'usuari i cobrir les necessitats de comunicació interna i externa, resulta indispensable disposar d'una infraestructura TIC eficient, actualitzada i ben gestionada.

Aquest servei té un caràcter transitori, ja que es fonamenta en el manteniment i suport de les infraestructures actuals del CPD de l'Institut. En paral·lel, s'està duent a terme un procés de modernització de les aplicacions corporatives crítiques, amb l'objectiu de preparar la seva migració progressiva als serveis en el núvol gestionats pel CTTI, en línia amb l'estratègia de transformació digital de la Generalitat de Catalunya. Aquesta doble línia d'actuació permetrà assegurar la continuïtat operativa durant el període de transició, tot garantint una evolució cap a un model més sostenible, flexible i alineat amb els estàndards tecnològics corporatius.

3 TERMINI DE PRESTACIÓ DEL SERVEI

La prestació del servei s'estructura en diferents períodes, segons el tipus de servei contractat:

- Els serveis professionals d'administració del CPD s'iniciaran l'1 de setembre de 2025 i finalitzaran el 31 de desembre de 2026.
- Els serveis de manteniment de maquinari, còpies de seguretat, així com el manteniment del sistema d'alimentació ininterrompuda (SAI), s'estendran des de l'1 de gener de 2026 fins al 31 de desembre de 2026.

No es preveu cap pròrroga més enllà d'aquest període, atès que el servei té un caràcter transitori, vinculat al procés de migració als serveis Cloud del CTTI, previst per a la seva finalització a finals de 2026, i a l'obsolescència prevista del maquinari actual del CPD, que en farà inviable la seva continuïtat més enllà d'aquesta data.

4 CONTINGUTS DEL SERVEI

A continuació es detallen les activitats a contemplar en el servei a prestar per l'empresa adjudicatària:

4.1 Gestió, operació i manteniment de les eines i plataformes associades a l'explotació de sistemes i infraestructures informàtiques del CPD

Té com a funció principal la supervisió, gestió i resolució d'incidències, principalment en remot, de tota la infrastructural informàtica del CPD de l'Institut, que dona servei als usuaris i a les seves aplicacions.

Aquesta infraestructura, la que principalment es troba instal·lada en una sala tècnica de l'edifici on resideix l'Institut actualment, està formada actualment per servidors de Correu, Active Directory, Virtualització VMWARE, Web, Linux, equipament de xarxa i comunicacions, equips de back-up, SAI, programari de seguretat, antivirus i anti-spam, i inclou les plataformes Windows Server, Exchange Server, Linux Ubuntu Server, Apache, VMWARE, ORACLE, MySQL, TOMCAT, utilitzades pels servidors (veure detall en annex I.B i I.C).

Per tant, aquest servei de gestió ha d'assumir les següents funcions:

- Monitorització i control dels servidors (rendiment, programari, etc.).
- Manteniment de la documentació relativa als procediments operatius.
- Gestió de permisos i accessos als recursos dels sistemes, garantint la seguretat segons els estàndards i directrius de l'Institut.
- Actualització dels sistemes operatius i programari de seguretat, renovació de llicències i generació de la documentació necessària que reflecteixi els canvis realitzats.
- Instal·lació i configuració de noves aplicacions i/o eines d'ús general d'acord amb els requeriments establerts per la gerència de l'Institut, l'empresa de desenvolupament i conforme al protocol establert per l'Institut per la posada en producció de nou programari.

- Gestió de l'emmagatzematge de dades. Planificació de la capacitat operativa del sistema. Optimització del rendiment dels sistemes.
- Manteniment correctiu i evolutiu de la plataforma.
- Col·laboració i assessorament tècnic a l'equip de desenvolupament per la implementació i posada en funcionament de nou programari vinculat a nous projectes de gestió de l'Institut (gestió documental, administració electrònica etc..).
- Consultoria en processos d'optimització de plataformes servidors.
- L'empresa adjudicatària s'encarregarà de la realització i supervisió de les còpies de seguretat dels sistemes i bases de dades de l'Institut, d'acord amb la política de seguretat establerta i la normativa de l'administració de la Generalitat de Catalunya.
- Referent a la instal·lació del CPD, l'adjudicatari assumirà l'operació i gestió tècnica de sistemes, realitzant el control, monitorització i operació de les consoles dels servidors, la monitorització del rendiment on-line i la resolució de problemes inherents al procés informàtic. Cal destacar les tasques següents:
    - Planificació i control d'explotació, que inclou la realització de treballs, i la generació de la documentació necessària.
    - Operació dels sistemes de Producció.
    - Verificació del correcte funcionament del CPD mitjançant la revisió dels logs generats pels sistemes operatius, les aplicacions i els processos.
    - Reinici de servidors, elements de xarxa i comunicacions.
    - Generació d'informes del servei.
- Dins d'aquesta operació i gestió del CPD, cal incloure un servei de guàrdia que consistirà en una bossa de tres serveis extres a l'any, per al cas que es produeixi un tall elèctric (imprevist o planificat) i que existeixi la necessitat de reiniciar els servidors. Les tasques a realitzar en el cas que es produeixin aquestes actuacions són les següents:
    - Si és una activitat planificada, realitzar l'aturada ordenada de tot l'equipament afectat, tenint sempre a mà la darrera versió dels diferents procediments per restaurar aquestes infraestructures
    - Si fos una fallida de la llum (tall general, problema al magneto, etc.), caldrà actuar per mirar de restablir el subministrament elèctric. En cas de que no sigui possible, posar-se en contacte amb l'empresa de manteniment de la línia de baixa tensió d'urgències.
    - Una vegada restablert aquest subministrament de corrent:
        - Iniciar els hosts virtuals i les cabines de backup
        - Revisar que els racks de xarxa i comunicacions inicïin correctament (revisar connectivitat de les diferents línies)
        - Iniciar les màquines virtuals, revisar que els serveis (telefonia, correu, internet i diferents aplicacions internes) funcionin correctament
    - Aquest servei, en cas de ser planificada la intervenció, es realitzarà fora de l'horari de l'Institut (de dilluns a dijous, a partir de les 20.00 hores fins les 8 hores de l'endemà, divendres a partir de les 19.00h, caps de setmana i festius).
- Suport oficina virtual: Aquest servei comprèn l'execució de les tasques següents:
    - Gestió dels subdominis oficinavirtual.llull.cat i oficinavirtual-d.llull.cat
    - Seguiment sobre el rendiment de les màquines oficinavirtual.llull.cat i oficinavirtual-d.llull.cat pel taulell de control de Swpanel.
    - Gestió d'usuaris, contrasenyes, bases de dades i comptes FTP sobre aquests subdominis pel taulell de control de Swpanel.

- Gestió de les peticions per part de l´empresa de desenvolupament sobre aquestes amb el hosting.
- Interlocució entre l'Institut i el hosting.
- Reunions periòdiques amb el proveïdor del hosting pel seguiment de les màquines, noves propostes, migracions.
- Suport i consultoria en el procés de migració cap a nous aplicatius i/o entorns de gestió de l'administració electrònica, segons instruccions de la gerència.

4.2 Manteniment del maquinari

L'objecte d'aquest apartat és establir les condicions tècniques per a la contractació d'un servei de manteniment preventiu i correctiu del maquinari físic ubicat al CPD de l'Institut. Aquest servei garantirà la continuïtat operativa i la resolució àgil d'incidències en el maquinari crític per al funcionament del CPD.

El servei inclourà com a mínim:

- Diagnòstic i resolució d'incidències de maquinari en servidors físics, cabines de discs, sistemes d'emmagatzematge i components associats.
- Subministrament i substitució de peces defectuoses o avariades.
- Suport tècnic remot i in situ 24x7 amb temps de resposta màxim de 4 hores naturals per a incidències crítiques.
- Assistència durant dies laborables i festius.
- Cobertura per a equips detallats en Annex I.A.

4.3 Còpies de seguretat i sistemes de recuperació davant desastres

L'objecte d'aquest apartat és contractar el servei de còpies de seguretat remotes per garantir la protecció i recuperació de la informació digital crítica de l'Institut mitjançant sistemes d'emmagatzematge fora de les instal·lacions del client, amb accés segur i supervisió contínua. El servei inclou:

- Plataforma de còpia de seguretat remota per transmissió xifrada via Internet.
- Almenys 3.000 GB d'emmagatzematge contractat, amb gestió d'excedents mensuals.
- Servidor de còpies local cedit en règim d'ús, amb manteniment integral inclòs.
- Gestió de l'ocupació i transmissions, amb:
  - Alertes d'error.
  - Informes diaris automàtics per correu electrònic.
  - Monitorització de l'estat i la integritat de les còpies.
- Suport tècnic regular (de dilluns a divendres de 8h a 18h) i servei d'emergència 24x7 per incidències crítiques.
- Recuperació de dades sota demanda, sense cost afegit si es fa via descarrega directa.
- Plataforma i interfície d'accés per a l'usuari, amb eines de consulta i gestió.
- El servei es prestarà amb mecanismes de xifratge i compressió, amb les claus gestionades únicament pel client.
- El proveïdor actuarà com a encarregat del tractament de dades, segons el Reglament General de Protecció de Dades (RGPD).

- El proveïdor haurà de signar i complir amb l'Acord d'Accés a Dades per compte de Tercers, inclòs com a annex.
- Els sistemes de còpia han de garantir:
  - Confidencialitat, integritat i disponibilitat de les dades.
  - Recuperació ràpida davant incidents.
  - Informes i evidències de compliment de la normativa.
- El proveïdor disposarà d'una pòlissa de responsabilitat civil vigent per a possibles pèrdues de dades, amb cobertura mínima de 600.000 €.
- El proveïdor haurà de disposar, en CPDs propis o de tercers, de la capacitat tècnica i logística per recrear l'entorn de producció de l'Institut Ramon Llull en un termini màxim de 48 hores en cas de desastre crític (Disaster Recovery as a Service). Aquesta recreació inclourà, com a mínim, les següents màquines virtuals:
  - Producció64 (aplicacions com Intrallull, viatges, biblioteca, formularis de RRHH, etc.).
  - Irlpro (instància de l'aplicació Alfresco).
  - Mysql64 i Irlbcn04 (bases de dades MySQL i Oracle).
- Aquesta capacitat haurà d'estar detallada en una proposta de pla de contingència, que inclogui:
  - Recursos disponibles per a la restauració (CPU, RAM, disc).
  - Procediment de restauració validat periòdicament.
  - Evidència documental de proves de recuperació (mínim un cop l'any).

4.4 Manteniment del sistema d'alimentació ininterrompuda (SAI) de la sala tècnica

L'objectiu d'aquest apartat és contractar el servei de manteniment preventiu i correctiu per al sistema d'alimentació ininterrompuda (SAI) del CPD de l'Institut Ramon Llull, per tal de garantir-ne la continuïtat operativa i el correcte funcionament elèctric i ambiental:

- **Model:** Symmetra PX 40kW Scalable to 40kW N+1
- **Número de sèrie:** PD0740360013

El servei inclourà com a mínim les següents prestacions:

- Manteniment preventiu anual, incloent inspecció visual, mecànica i elèctrica, verificació de registres d'alarmes, proves funcionals i actualitzacions de firmware si s'escau.
- Monitorització remota 24/7/365 i assistència tècnica 24/7 amb servei tècnic in-situ l'endemà (amb opcions d'escalat a 8 o 4 hores).
- Diagnòstic i reparació de l'equip per personal certificat del fabricant, amb desplaçament inclòs.
- El proveïdor estarà obligat a complir amb la normativa de seguretat i accés a les instal·lacions segons indicacions del centre.
- El proveïdor haurà de lliurar un **informe anual complet** amb les proves i accions realitzades.
- Es designarà un interlocutor tècnic de l'organització per a la coordinació del servei.
- L'empresa adjudicatària haurà de conservar les evidències de totes les actuacions per a possibles auditories.

4.5 Qualitat i auditoria del servei

La finalitat d'aquest servei és mesurar, analitzar i reportar la qualitat del servei adjudicat. Aquest servei es prestarà amb els recursos del servei continu dimensionat correctament per tal de poder assolir les funcions assignades.

Pel que fa a les auditories de qualitat, seran necessàries com a mínim auditories de dues tipologies:

- Realitzades per la mateixa empresa adjudicatària, periòdiques i puntuals sobre totes les parts del servei. L'empresa adjudicatària presentarà i lliurarà els informes d'auditories internes realitzades amb la periodicitat que es pacti amb l'Institut. Exemples de parts del servei a auditar per la mateixa empresa adjudicatària són: qualitat de l'atenció telefònica de tots els agents del servei en referència al tracte a l'usuari, el coneixement de les operatives i procediments que fan referència a les eines per part dels agents, qualitat de l'inventari dels elements dels usuaris a les eines, qualitat de l'entrega de servei per part dels tècnics. Aquest servei es prestarà amb els recursos del servei continu dimensionat correctament per tal de poder assolir les funcions assignades.

- Planificades per l'Agència de Ciberseguretat (GDPR, ENS, Marc normatiu, tècnica) per verificar el compliment dels requisits de seguretat de l'empresa adjudicatària, del servei prestat i nivell de compliment del marc normatiu de seguretat de la Generalitat. Concretament, es podrien dur a terme:
  - Auditoria GDPR/ENS/Marc Normatiu: lliurament de les evidències en temps i forma.
  - Auditoria tècnica: lliurament d'un equip tipus amb totes les polítiques i mesures de seguretat desplegades per la seva avaluació.

4.6 Seguretat

Addicionalment als requeriments de seguretat inclosos en la descripció de cadascun dels serveis vinculats a l'entrega de serveis, en aquest apartat es remarquen aquells requeriments de seguretat que són transversals a tots ells i de major rellevància.

A tal efecte, durant els tres primers mesos del servei, l'empresa adjudicatària haurà de desenvolupar i presentar un pla de treball inicial (Pla de Seguretat) per desplegar els serveis de seguretat descrits en l'annex I.C que, conjuntament amb l'Institut, s'acordin com més crítics en tot allò que correspongui a les funcionalitats i responsabilitats atribuïdes a l'empresa adjudicatària dins l'àmbit de manteniment i administració dels equips del CPD. L'Agència de Ciberseguretat de Catalunya determinarà el nivell de compliment exigible segons el grau d'accés, impacte i riscos derivats del servei.

Aquest pla de seguretat s'utilitzarà per fer el seguiment de l'evolució del desplegament així com per incorporar tot allò que es vagi desenvolupant durant l'execució del contracte. Al final del contracte o de les seves pròrrogues, caldrà lliurar un informe (memòria) sobre l'assoliment d'aquest pla incorporant les accions desenvolupades.

Per tant, amb aquest pla de seguretat es busca:

- La incorporació al model de compliment normatiu de la Generalitat, que porta a terme l'Agència de Ciberseguretat per tal d'assolir el compliment del Marc Normatiu de seguretat de

la informació de la Generalitat de Catalunya (en endavant, marc normatiu de seguretat) i la legislació i estàndards vigents[1] en tots aquells aspectes relatius a la seguretat.

- La implantació dels controls de seguretat que permetin mitigar els riscos als que estan exposats els sistemes d'informació i processos objecte del contracte, així com l'adopció del model d'arquitectura de ciberseguretat i el desplegament del perímetre de ciberseguretat definits per l'Agència de Ciberseguretat de Catalunya.
- La coordinació i integració operativa segons el model operatiu de ciberseguretat de l'Agència de Ciberseguretat de Catalunya, amb els diferents serveis de prevenció, detecció, protecció i resposta de l'oficina QA de Ciberseguretat i l'Agència de Ciberseguretat per fer front a situacions d'amenaça o davant incidents de seguretat que afectin als actius objecte del contracte.
- Que l'empresa adjudicatària sigui coneixedora en tot moment de les principals amenaces de seguretat que poden afectar el lloc de treball, amb la finalitat d'implantar les mesures pertinents per fer-hi front i reduir el nivell d'exposició i de risc a un nivell acceptable pel negoci.
- Atesa la naturalesa canviant de les amenaces de seguretat, la pròpia evolució tecnològica i els canvis que es puguin produir en la prestació del servei, l'empresa adjudicatària haurà d'adequar els controls, les mesures de seguretat i el servei prestat per fer front a aquestes noves amenaces, als canvis tecnològics i als canvis en la forma de desplegar el servei que es puguin esdevenir durant l'execució del contracte. De forma general, és fonamental que les mesures de seguretat a desplegar permetin fer front a, com a mínim, amenaces del tipus:
  - Robatori d'informació, amb el posterior impacte al negoci i legal (com la RGPD).
  - Intrusió als equips, canvis de configuració/seguretat per agafar-ne el control. Per exemple, pel desplegament de codi maliciós o connexions C&C que permetin controlar l'equip remotament, desplegament de software espia (spyware), software d'actualització maliciós (rogue security software).
  - Ús de mecanismes d'identificació i autenticació insegurs. En aquest cas, l'ús de contrasenyes febles o l'ús de contrasenyes corporatives en entorns no corporatius, podria facilitar l'accés per part d'un atacant.
  - Robatori de credencials dels usuaris. Per exemple, per l'enviament de phishing als usuaris.
  - Pèrdua o robatori dels equips, que pot implicar l'accés a informació confidencial o sensible guardada a l'equip.
  - Explotació de les vulnerabilitats dels equips de lloc de treball. Per exemple, vulnerabilitats del sistema operatiu, dels servidors (AD, Printing, concentrador VPN, etc.), que poden derivar en altres amenaces.
  - Interceptar el tràfic de xarxa per la captura d'informació que s'envia des de o cap als llocs de treball (DNS spoofing, HTTPS spoofing, WIFI hacking, SSL hacking, entre altres).
  - Accés a la xarxa de la Generalitat aprofitant les vulnerabilitats dels equips. Els atacants podrien aprofitar les vulnerabilitats dels equips (VPN, directoris actius obsolets, sistemes operatius sense suport, etc.) per accedir a la xarxa corporativa amb la finalitat de portar a terme un atac informàtic de més envergadura.
  - Denegació dels serveis de DNS i DHCP.
  - Incompliment legal. Per exemple, incompliment de la RGPD per accés a dades personals dels usuaris (robatori de credencials dels directoris actius de lloc de treball, per exemple).

[1] Els estàndards vigents es podran consultar al portal de seguretat de l'Agència de Ciberseguretat: https://portal.cesicat.cat (àrea pública).

- Provocar una denegació del servei de lloc de treball. Per exemple, xifrat dels equips (ransomware), infecció de la xarxa, atac informàtic dirigit, etc.
- Accés a la xarxa de lloc de treball i als equips per part d'administradors no autoritzats o per un ús il·legítim. Ús no autoritzat de recursos.
- Errors dels administradors del servei. Per exemple, configuracions errònies, mesures de seguretat mal aplicades, etc.
- Accessos remots no controlats per fer el manteniment dels equips. Els atacants podrien aprofitar mecanismes d'accés remot febles (per exemple, VPN amb contrasenyes febles, RDP activat sense control, ús de eines de control remot vulnerables, etc.).
- Enginyeria social per accedir a informació confidencial del personal que presta el servei.

Aquest servei (redacció i seguiment del pla de seguretat) es prestarà amb els recursos del servei continu dimensionat correctament per tal de poder assolir les funcions assignades, si bé l'execució dels projectes que es derivin del pla s'hauran d'executar amb els recursos addicionals especialitzats que s'acordin amb l'institut.

5 DIMENSIONAMENT DEL SERVEI

5.1 Mitjans humans

Per la prestació del servei, i considerant el parc i l'activitat detallada en:

- Annex I.A Equipament del centre de procés de dades (CPD)
- Annex I.B ANS dels serveis

S'ha estimat que les hores que es consumiran d'aquest servei serà igual als equivalents a temps complet – ETC (1.700 h/any) següents, per a cada perfil professional:

Costos directes de mà d'obra (durada total del contracte)	Hores totals	ETC (16 mesos)
Administrador/a	90	0,04
Tècnic/a de plataforma / Explotació / Supervisor/a	240	0,11
Operador/a de SAU (nivell 2)	270	0,12
TOTAL	**600**	**0,27**

L'empresa adjudicatària assignarà els tècnics necessaris considerant un mínim de quatre anys d'experiència en llocs similars, i amb coneixements amplis de les plataformes i servidors que s'utilitzen a l'Institut (VMWARE, Ubuntu, Windows Server, Exchange Server, Linux Apache, MySQL, TOMCAT i especialment en l'administració de base de dades ORACLE).

L'empresa adjudicatària pot proposar el canvi dels tècnics assignats a l'Institut amb un preavís de 15 dies i justificant el motiu del canvi. Sempre que es produeixi un canvi de tècnic, haurà de coincidir amb l'anterior almenys 5 dies, per poder fer el traspàs de la informació referent al servei.

Caldrà preveure que, sempre que les circumstàncies associades a les tasques a realitzar així ho requereixin, el personal del servei de gestió sistemes s'haurà de desplaçar a la seu del Consorci a Barcelona, prèvia comunicació a l'Institut, per tal de gestionar la seva ubicació i la disponibilitat dels mitjans auxiliars necessaris (taula, cadires, etc..).

L'empresa adjudicatària es responsabilitzarà de la formació continuada de tots els tècnics assignats per tal que portar a terme la correcta realització dels serveis que es contracten i la seva evolució.

5.2 Àmbit i horari de cobertura del servei

Els horaris de cobertura mínima per la prestació dels diferents serveis es detallen a continuació:

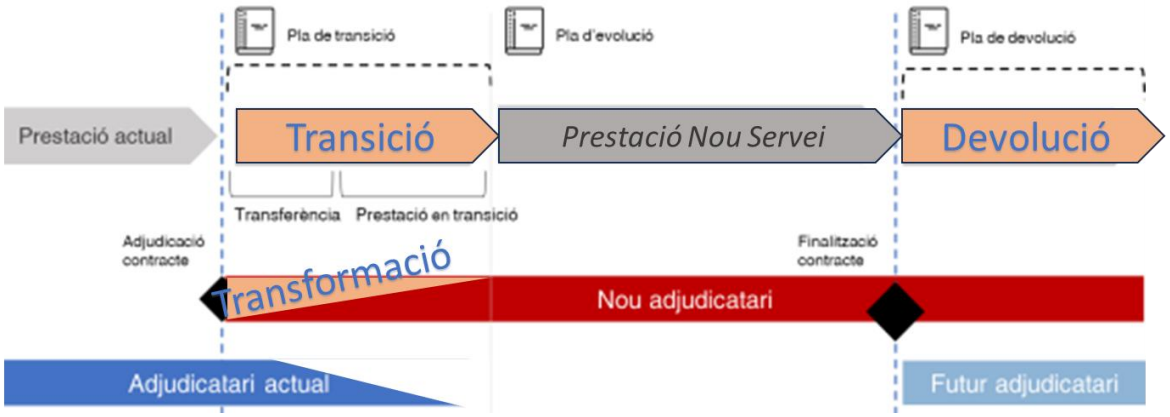
- Servei de gestió i operació remota de les infraestructures (12 mesos/any):
  - Horari de 8h a 20h tots els dies laborables segons el calendari festius de la província de Barcelona.
  - Atendrà tant les trucades dels usuaris de les oficines centrals de la seu de l'Institut a Barcelona, com les trucades de les diferents delegacions i personal desplaçat.
- Per la resta des serveis detallats en aquest plec, en tractar-se de components de gestió i coordinació, no es fixa cap horari concret, però si que cal disponibilitat per desplaçar-se puntualment a les oficines de l'Institut per participar en reunions de seguiment, presentació d'iniciatives de millora, etc.

6 FASES DE LA PRESTACIÓ DEL SERVEI

En aquest capítol es dona una explicació de les fases per les que passarà el cicle de vida del contracte objecte d'aquest plec. Concretament, es consideren com a fases d'aquest cicle de vida les següents:

- La fase de Transició (en cas que es produeixi un canvi de proveïdor respecte l'actual).
- La fase de Transformació.
- La fase de Prestació del Nou Servei.
- La fase final de Devolució.

En el següent esquema (no proporcional a les durades previstes) es presenta la seqüència d'aquestes fases:



En el següents apartats es donen explicacions de les particularitats de cadascuna d'elles, a excepció de la fase de prestació del nou servei, detallada àmpliament en els capítols anteriors.

6.1 Transició del servei entre proveïdors

És el període que va des de l'adjudicació del contracte a un nou proveïdor fins a l'estabilització dels serveis en els nivells que el prestador sortint els estava donant prèviament. Per tant, té per objectiu donar continuïtat al servei existent, desenvolupant les activitats necessàries per assumir el coneixement i minimitzant l'afectació d'aquest traspàs.

La transició es considerarà finalitzada quan sigui aprovada per l'institut.

Durant la fase de transició es diferenciaran dues etapes:

- **Transferència**: El nou adjudicatari es posarà en contacte amb l'actual per planificar les tasques de traspàs de coneixement i l'habilitació de l'operació. Durant aquesta fase, l'actual adjudicatari continuarà prestant el servei. La transferència entre proveïdors serà responsabilitat del proveïdor entrant, tot i que el proveïdor sortint ha de col·laborar perquè, en cap cas, aquesta transferència afecti el funcionament del servei. Per garantir aquesta col·laboració, l'Institut supervisarà els processos de transferència del coneixement que han d'incloure, almenys:
  - Assignació de recursos. El proveïdor entrant ha de comunicar a l'organització amb què proporcionarà el servei, així com l'assignació de recursos i confirmació de rols, tasques i responsabilitats necessàries per a la prestació del servei.
  - Formació específica i formal per a l'assumpció del servei. Aquesta formació serà proporcionada pel proveïdor sortint segons les condicions que hagi acordat amb el proveïdor entrant del servei i sota la supervisió de l'Institut.
  - La documentació necessària per a l'assumpció del servei ha ser proporcionada pel proveïdor sortint. És responsabilitat del proveïdor entrant identificar, demanar i recopilar tota la informació necessària per a la correcta prestació del servei (documentació dels equips, sistemes i aplicacions, documentació tècnica, procediments d'actuació, entre d'altres). En aquells casos en què no hi hagi documentació prèvia necessària per prestar el servei, el proveïdor haurà de planificar i executar la seva elaboració, d'acord amb l'Institut i sense cost addicional.

La temporització d'aquesta transferència entre proveïdors es regiria segons les directrius següents:

- Presa de contacte: Es tracta d'una fase de durada curta que no ha d'excedir els cinc dies hàbils i que només es podrà prolongar en casos excepcionals (per exemple, per limitacions temporals en la implantació d'infraestructura o altres temes logístics). En aquest cas, se superposarà amb la fase de desenvolupament de la transferència, encara que sempre haurà de finalitzar abans de la transferència de responsabilitat. El proveïdor entrant haurà d'agilitzar, en aquest cas, la realització de totes les tasques associades per assegurar la consecució en temps de les fites planificades.
- Desenvolupament de la transferència de coneixement: L'objectiu d'aquesta fase és el traspàs dels elements bàsics i imprescindibles entre el proveïdor sortint i l'entrant per a la prestació del servei, i amb una durada no superior a quatre setmanes.

Un cop finalitzada la transferència, el proveïdor sortint finalitza les seves responsabilitats i és el proveïdor entrant l'únic responsable del servei a tots els efectes.

- **Prestació en transició**: El nou adjudicatari comença a prestar el servei amb els seus propis mitjans tal i com ho feia el proveïdor sortint, i passa a ser l'únic responsable de la prestació del servei. Aquesta prestació del servei no es pot veure afectada pel Pla de Transformació que es detalla més endavant.

Aquesta cooperació entre proveïdors té com a objectiu assegurar que no hi hagi interrupcions significatives en la prestació dels serveis de manteniment TIC i que es mantingui la qualitat i la eficiència dels serveis durant aquesta transició.

6.2 Pla de transformació del model de servei

L'empresa adjudicatària haurà de presentar un pla de transformació del model actual al nou model de servei seguint els principis descrits en el capítol 2 d'aquest plec, pla que haurà presentar les característiques següents:

- La durada del pla de transformació no excedirà, en cap cas, el termini màxim de tres mesos des de la data d'adjudicació.
- El pla de transició ha de garantir que no hi haurà cap interrupció del servei i per tant, ha de plantejar tots els mecanismes necessaris de traspàs d'activitats, desplegament eines, gestió de canvi, formació als usuaris, etc.
- Per a cadascuna de les tasques a dur a terme en aquest pla de transició, s'haurà de detallar:
  - Les dates d'inici i fi de totes les tasques, la distribució de responsabilitats, els criteris aplicables d'acceptabilitat i qualsevol altre detall addicional que s'estimi pertinent.
  - Planificació de la incorporació de recursos humans i materials al servei. Al respecte, es valorarà la disponibilitat per part dels licitadors de poder disposar d'una eina temporal de suport al SAU pel registre de l'activitat. L'objectiu de l'Institut és disposar d'una eina pròpia, però la seva selecció i desplegament es preveu a partir del segon trimestre del 2024.
  - Pla d'activació de cada servei, explicant l'impacte percebut per l'Institut i els plans de gestió del canvi associats.

- Identificació de riscos principals i el seu pla de resposta.
- Mètode de gestió de treballs en curs, entesos com aquelles activitats o tasques que estan iniciades o previstes al moment en què el proveïdor entrant assumeix la responsabilitat del servei.

Les empreses interessades en licitar que tinguin dubtes en relació amb el model actual de prestació de serveis podran plantejar les qüestions pertinents. Per tal de mantenir la transparència i igualtat entre els licitadors, l'Institut publicarà totes les preguntes i respostes a l'espai "anuncis" de la PSCP.

6.3 Pla de devolució del servei a la finalització del contracte

El licitador haurà de presentar un pla de devolució del servei detallat, que descrigui les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts i les condicions en que es realitzarà aquesta devolució a la finalització del contracte objecte d'aquest plec.

En cas de cessament o finalització del contracte, el proveïdor estarà obligat a tornar el control dels serveis objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb els de prestació del servei, sense cost addicional per l'Institut. Això ha de permetre licitar novament el servei en igualtat de condicions per a tots els licitadors que es vulguin presentar, evitant que l'empresa sortint pugui fer un mal ús de la seva posició de domini a la finalització del contracte.

Els objectius que es pretenen assolir amb el pla de devolució són:

- Garantir l'adequada transferència de coneixement sobre els usuaris, serveis, infraestructura i model de gestió vigents al proveïdor receptor.
- Assegurar la nul·la afectació al servei dels usuaris en el procés de devolució, mantenint el nivell de servei acordat i indicat en els Acords de Nivell de Servei (ANS).
- Ajustar els temps associats a la transferència de la infraestructura, dels serveis i de la seva gestió a la nova empresa homologada en els terminis prefixats.
- Per tal d'evitar que el proveïdor que estigui prestant el servei pugui fer un mal ús de la seva posició de domini a la finalització del contracte, estarà obligat a:
  - Utilitzar tecnologies i sistemes que no dificultin o impedeixin, a una nova empresa homologada, la continuïtat del servei i la seva gestió i explotació.
  - Facilitar tota la documentació, tant tècnica com administrativa, necessària per a realitzar el traspàs del servei, en un termini màxim de quatre setmanes després de la seva sol·licitud.
  - No dificultar el procés de canvi, ni degradar els ANS durant el procés de transició.

Al respecte, els licitadors hauran d'incloure en la seva oferta un pla de devolució del servei en què hauran de concretar les activitats de transferència del servei i del coneixement a un tercer proveïdor a la finalització del contracte.

El Pla de devolució haurà de complir, com a mínim, els següents principis i continguts:

- El termini d'execució serà de tres mesos des de la notificació oficial d'expiració o cancel·lació, total o parcial del servei. La durada concreta dependrà de la complexitat de cada servei. L'Institut es reserva el dret de poder reduir el termini d'execució segons consideri necessari.

- L'empresa adjudicatària haurà d'oferir tota l'ajuda en la transferència a terceres parts tant de serveis subcontractats, com de garanties o contractes de manteniment existents fins al moment de la terminació en els mateixos termes pactats amb les empreses implicades.
- Inclourà la metodologia de transferència de coneixement dels aspectes fonamentals d'operacions i projectes en curs i que, com a mínim, descriurà:
    - L'assistència, la formació i la documentació sobre els procediments de negoci o sistemes de l'Institut a la nova empresa adjudicatària.
    - L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat en la provisió del servei per l'empresa sortint.
- El pla de devolució ha de garantir que no es causa cap discontinuïtat en el servei ni en els seus nivells de qualitat.

Un cop finalitzat el procés de devolució del servei el proveïdor sortint haurà de prestar a l'Institut, dins del servei i terminis de la garantia establerta per l'adjudicació, serveis d'assistència, sense cost addicional, per resoldre les deficiències i/o mals funcionaments imputables a la seva actuació mentre hagi estat al capdavant del servei.

7 PROCEDIMENT D'AVALUACIÓ I CONTROL

El/la responsable del servei de l'Institut acordarà un calendari de reunions mensuals amb el/la Coordinador/a del servei de l'adjudicatari a l'efecte de controlar periòdicament l'execució del serveis prestats i de la satisfacció dels usuaris de l'Institut. En aquesta reunió es procedirà a l'examen i revisió del compliment de totes les condicions d'execució del contracte fixades en aquest plec a partir del informe mensual que, entre altres, ha de presentar una relació d'incidències i peticions gestionades i del nivell de compliment dels ANS associats a ser possible segmentades per àrea de l'Institut

En aquestes reunions es realitzarà un acta resum dels temes tractats, on també hi recollirà les propostes de solucions i/o millores per tal de suprimir la incidència o incidències trobades, durant el nou període d'execució. La solució/millora proposada serà el resultat del debat i consens entre el responsable del contracte i el representant de l'empresa contractista.

De totes maneres, es dona llibertat als licitadors a presentar en els annexos de les seves ofertes exemples d'informes de seguiment que es proposaran per aquestes reunions mensuals, tenint sempre present que la llengua vehicular dels informes ha de ser el català.

8 REQUERIMENTS DE L'ADJUDICATARI

L'empresa adjudicatària haurà de comptar amb els següents certificats, com a requisits de solvència tècnica i professional previstos a l'Annex II del Plec de clàusules administratives particulars:

- Disposar de la certificació oficial com a partner de VMware (nivell Professional Partner o superior).
- Disposar de la certificació oficial com a partner de Veeam (nivell Silver Partner o superior).
- Disposar de la certificació oficial com a partner de Microsoft, en alguna de les categories següents: "Microsoft Solutions Partner" o certificació equivalent reconeguda.

- Disposar de la certificació oficial com a HP Business Partner o equivalent, que acrediti capacitat per mantenir equips físics HP (servidors i emmagatzematge).
- Certificació ISO 9001 de qualitat o equivalent.
- Certificació ISO 14001 de gestió mediambiental o equivalent.
- Certificació ISO 20000 de gestió de serveis TIC o equivalent.
- Certificació ISO 27001 relativa als Sistemes de seguretat de la informació o equivalent.
- Certificació dels coneixements i experiència dels tècnics de nivell superior en Windows Server, Exchange Server, Linux Apache, VMWARE, MySQL i especialment en l'administració de base de dades ORACLE.

ANNEX I.A - Equipament del CPD i activitat associada

Servidors físics: Hi ha un total de 2 servidors Hp Proliant dl 360 gen 10. Estan dedicats a la virtualització i allotgen 20 servidors virtuals, amb possibilitat de creixement.

Es disposa d'un **sistema d'emmagatzematge i còpies** de seguretat amb el següents elements:

- Hp Proliant DL 380 Gen9

- HP MSL 2024

- Nas DS916+

Sistemes operatius dels servidors:

- Windows Server 2003, 2012, 2016, 2019
- Exchange Server 2016,2019 office 365
- Linux Ubuntu 10.04, 20.4
- Centos

Entorn de virtualització: VMWARE 7.0.3.01100

Gestor documental: Alfresco Community v5.2.0

Programari de backups: Veeam backup & Replication 11 build 11.0.1.1261

Altre programari:

- Programari de catalogació de biblioteques: Coeli
- Programari antispam: GFMAIL
- Eina de monitorització i control d'incidències: KASEYA
- Programari de BBDD: Oracle Sql Server v19 i Mysql 5.1.41
- Entorn de desenvolupament: Java/JSP 1.7.0.80 , PHP 5.3.2-1

Servidors Virtuals

Denominació	Descripció	Sistema Operatiu	CPU MHz	Memòria MB	DISC GB
Desenvolupament64	Desenvolupament64 : Servidor Ubuntu que utilitza IThinkUPC per desenvolupar els diferents projectes de l'Institut.	Ubuntu Linux (64-bit)	20	81	32,1
Irlbcn04	Irlbcn04: Servidor Windows on està l'aplicació Sicap i Oracle.	Windows Server 2003	460	240	89,04
Irlbcnsql	Irlbcnsql: Servidor amb sql server 2019 per aplicació Evalos i aplicació precisió CPD.	Windows Server 2016	83	614	77,31
Irlpro	Irlpro: servidor amb Ubuntu 20.04 amb aplicació alfresco	Ubuntu Linux (64-bit)	481	1,56	112
Mysql64	MySQL64: Servidor Ubuntu que conté les bbdd on apunta la màquina de producció (intrallull, alfresco, Venecià...)	Ubuntu Linux (64-bit)	62	798	606
Producció64	Producció64: Nou servidor Ubuntu on està allotjat l'Intrallull i que conté les aplicacions de viatges, biblioteca, formularis rrhh, etc.	Ubuntu Linux (64-bit)	41	184	36
Irldades01	Irldades01: Servidors de dades exclusiu per SICAP	Windows Server 2019	41	901	432
GLPI	GLPI: Servidor on esta l'eina de ticketing GLPI	Ubuntu Linux (64-bit)	41	163	18
GLPI2	GLPI2 : Plugins estadístiques GLPI	Ubuntu Linux (64-bit)	21	10	1
Irlad01	Irlad01: servidor d'Active Directory	Windows Server 2016	125	983	67,62
Irlad02	Irlad02: servidor DNS secundari	Windows Server 2016	41	983	71
Irlex04	Irlexchange04: Nou servidor de correu actualitzat a exchange2016	Windows Server 2016	523	5,28	271
Vcenter2022	Irlvcenter: Servidor Windows per gestionar les màquines virtuals	VMWare Photon	293	4,37	222
IrlVeeam01	Veeambackup: Servidor que realitza les còpies de seguretat de les màquines virtuals	Windows Server 2016	543	1,28	122
Zabbix	Monitorització principals alarmes	Debian GNU/Linux 11	1,11	983	71,51

Detall de les principals activitats:

Tipus d'activitat	Subtipus / Descripció	Sistema / Àmbit	Freqüència habitual	Observacions
Manteniment preventiu	Revisions de maquinari físic	Servidors físics	Eventual	Segons disponibilitat d'intervenció
Supervisió d'estat	Monitoratge de serveis i sistemes	Virtualització, Veeam	Diària	Automatitzada
Gestió d'incidències	Resolució correctiva	Qualsevol sistema afectat	Discrecional	Mitjana de 10-12 per mes
Còpies de seguretat	Verificació correcta	Veeam	Setmanal / Trimestral	
Gestió de recursos	Ampliació de disc, memòria, etc.	Entorns virtuals	Eventual	Segons creixement de recursos de les màquines virtuals
Suport tècnic puntual	Consultes, assistència	Xarxa, Antivirus	Discrecional	
Actualitzacions SW/HW	Pegats, firmware	Host ESXi, SAI, switches	Eventual	Segons actualitzacions disponibles
Informes i seguiment	Enviament a client / reunions tècniques	Tots	Mensual	Inclou imatges estat dels recursos de las màquina, incidències i manteniment preventiu

ANNEX I.B - Acords de nivell de Servei (ANS)

L'empresa adjudicatària ha d'executar el contingut d'aquest contracte, a la finalització de l'etapa de transició, d'acord amb els ANS de les taules següents:

Manteniment Correctiu:

Codi	Nom de l'Indicador	Valor Objectiu	% Mínim de Compliment	Límit compliment
MC1	Temps de resposta a incidències crítiques	15'	90%	<=30'
MC2	Temps de resposta a incidències no crítiques	2 hores	90%	<=4h
MC3	Temps de resolució a incidències crítiques	8 hores naturals	90%	<=48 h naturals
MC4	Temps de resolució d'incidències no crítiques	12 hores laborals	95%	<=4 dies laborables
MC5	Disponibilitat del servei	97,5% temps		>=90%
MC6	Índex de reobertura d'incidències	0 reobertures	90%	<= 3 reobertures

Tenen **consideració de crítiques** les incidències que facin referència a: Usuaris VIP (Director/a, el/la Gerent i Directors/es d'Àrea) i claus (Gestió Econòmica i Recursos Humans), o incidència que impliqui una aturada o un funcionament inferior als estàndards de qualitat en l'operativitat diària i normal d'un grup d'usuaris. També són crítiques les incidències que ocorrin els dies en què acaben terminis de procediments i les relacionades amb els òrgans de govern de l'Institut (Consell de Direcció i Junta Rectora).

La penalització associada als incompliments serà d'1% de la facturació per cada 1% diferencial respecte els llindars fixats, i en cap cas superarà el 10% de la facturació mensual, tot i que l'acumulació d'incompliments per sobre del 10% durant 3 mesos seguits podrà ser motiu per rescindir el contracte.

De totes maneres, aquest mecanisme de penalitzacions solament es farà efectiu a partir que s'acordi entre l'Institut i l'adjudicatari en acta formal dins del seguiment mensual i que les eines i procediments existents permetin obtenir una visió objectiva del servei.

ANNEX I.D – Marc del Model de Seguretat a considerar

L'empresa adjudicatària haurà d'incorporar, en els serveis prestats, el model de compliment normatiu de la Generalitat, que porta a terme l'Agència de Ciberseguretat. En aquest model s'integren les possibles auditories que l'Agència de Ciberseguretat determini realitzar, així com el seguiment dels plans d'acció derivats de les mateixes. També s'inclou en aquest model el compliment per part de l'empresa adjudicatària de plans d'acció relatius a normatives o estàndards que l'Agència de Ciberseguretat determini realitzar i el seu seguiment recurrent. Així mateix, l'empresa adjudicatària haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en el model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. La gestió del compliment es realitzarà amb l'eina que determini l'Agència de Ciberseguretat.

En els casos que l'Agència de Ciberseguretat determini, l'empresa adjudicatària instal·larà eines automàtiques indicades per l'Agència de Ciberseguretat, per auditar el grau de compliment normatiu de forma contínua i automàtica.

L'empresa adjudicatària haurà de garantir que l'entorn de treball compleix amb les normes de bastionat establertes per la Generalitat.

L'empresa adjudicatària haurà de garantir l'accés del personal autoritzat de l'Agència de Ciberseguretat a la informació de seguretat (procediments, registre d'incidents, traces, etc.). Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'Agència de Ciberseguretat i l'empresa adjudicatària estabiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

En relació al tractament de dades de caràcter personal, l'empresa adjudicatària donarà compliment com a encarregat de tractament a allò establert al Reglament General de Protecció de Dades. Pel que fa la seguretat en el tractament de les mateixes, l'empresa adjudicatària implementarà les mesures de seguretat establertes per l'Agència de Ciberseguretat en el Marc de Ciberseguretat per a la Protecció de Dades. Aquesta implementació i nivell de compliment seran incorporats al model de compliment normatiu de la Generalitat de Catalunya.

En cas d'execució d'auditories i seguiment dels plans d'acció derivats, aquestes hauran de realitzar-ne amb la metodologia i eines establertes per l'Agència de Ciberseguretat.

Gestió d'excepcions de seguretat l'empresa adjudicatària haurà de:

- Fer un seguiment continu de les excepcions de seguretat a les quals es veuen afectats els serveis objecte del contracte.
- Elevar riscos als comitès de seguiment en relació a excepcions considerades de risc alt, per assegurar la seva gestió i seguiment.
- Garantir que un cop les excepcions hagin expirat, es procedeixi a eliminar la mesura d'excepció. Per exemple, exceptuar temporalment el filtrat de navegació per un grup d'usuaris amb necessitats especials degudament justificades. Des de l'Agència de Ciberseguretat hauran d'autoritzar de forma expressa aquestes eliminacions.

Gestió de Traces

L'empresa adjudicatària haurà de complir amb la norma de gestió de traces vigent. L'empresa adjudicatària haurà de proveir d'un repositori de traces, on es guardin les traces de tots els serveis prestats (accessos, canvis de configuració, etc.) i assegurar que emmagatzema totes les traces que li són d'aplicació d'acord al marc normatiu i legal aplicable. L'empresa adjudicatària haurà de presentar un pla d'adequació al compliment de la norma de traces en els primers tres mesos a partir de la data d'adjudicació del contracte i fer-se efectiu en un període inferior a un any.

Les traces hauran de ser accessibles en mode lectura per a que puguin ser integrades amb el repositori de traces de seguretat de l'Agència de Ciberseguretat.

Seguretat en el núvol

Al igual que les aplicacions emmagatzemades on-premise, totes les aplicacions i contenidors del núvol (cloud) hauran de complir els requeriments de seguretat que estableix el marc normatiu de seguretat, els quals seran revisats per l'Agència de Ciberseguretat.

Operacions de ciberseguretat

L'Agència de Ciberseguretat disposa d'un model d'operació de la seguretat amb l'objectiu assolir un nivell de seguretat als àmbits adequat (inclòs el lloc de treball) i una clara coordinació operativa entre les parts. En aquest apartat s'exposen quins són eixos clau del model, fent focus en els processos clau, el model d'arquitectura, el model operatiu així com les principals funcions operatives que cal contemplar en el servei. Aquest model estarà a disposició de l'empresa adjudicatària en tot moment.

Els principals processos en l'àmbit de l'operació de la ciberseguretat són: la gestió de vulnerabilitats, la gestió d'amenaces i la gestió dels incidents de seguretat.

Per fer front a noves ciberamenaces vinculades al lloc de treball, l'Agència de Ciberseguretat ha definit un model d'arquitectura de seguretat específic pel lloc de treball.

Els elements principals que conformen aquest model d'arquitectura són:

- Les principals funcionalitats de seguretat a desplegar en l'àmbit dels diferents dispositius (portàtils, equips de sobretaula, mòbils, tauletes, etc.) i entorns que conformen el lloc de treball.
- El model d'administració de les funcionalitats que conformen el model d'arquitectura.
- El model d'integració operatiu de les esmentades funcionalitats de seguretat amb els sistemes de gestió de l'Agència de Ciberseguretat.

A l'inici de la prestació del servei, l'Agència posarà a disposició de l'empresa adjudicatària el model d'arquitectura per:

- Desplegar de forma efectiva el model als diferents entorns (equips de l'usuari, servidors, controladors de domini, directori únic, etc.).
- Operar, en els casos que sigui d'aplicació, les diferents solucions de ciberseguretat que composen el model d'arquitectura.

- Integrar els elements d'administració i gestió de les solucions de ciberseguretat que composen l'arquitectura amb els diferents òrgans especificats per l'Agència, els quals com a norma general podran ser:
  - Oficina QA de ciberseguretat. o Sistemes d'administració de la ciberseguretat del SOC de l'Agència (SIEM, SOAR, Data Lake, etc.).
  - Sistemes d'anàlisi de dades de l'Agència.

Model operatiu

L'empresa adjudicatària haurà de seguir el model operatiu definit per l'Agència de Ciberseguretat (basat en l'estàndard NIST SP 800-53) per la coordinació operativa amb totes les parts implicades en la operació de la ciberseguretat. Aquest model serà proporcionat per l'Agència a l'inici del servei. Les seves funcions són:

- Prevenció:

  - Desplegament dels pegats de seguretat dels fabricants de dispositius per la correcció de vulnerabilitats detectades sobre els dispositius objecte de la licitació, d'acord als terminis fixats pel Marc Normatiu, als nivells de servei sol·licitats en el contracte i al grau d'exposició que suposen aquestes vulnerabilitats.
  - Esborrat segur de tots els dispositius que siguin reutilitzats o que es vulguin donar de baixa d'acord al marc normatiu de la Generalitat, i en cas de baixa definitiva, aplicació dels procediments de destrucció segura corporatius així com el lliurament d'un certificat que ho certifiqui.
  - Execució dels plans de prova de seguretat dissenyats per l'Oficina de QA de ciberseguretat.
  - Pel que fa a la solució d'escaneig desplegada, serà responsabilitat de l'empresa adjudicatària el desplegament i manteniment dels agents desplegats en el diferents equips i infraestructura que conforma el lloc de treball.
  - Lliurament d'informes vinculats a les mesures de prevenció, com:
    - Calendari d'escanejos.
    - Inventari vulnerabilitats per cada actiu escanejat.
    - Pla d'acció per la gestió de les vulnerabilitats.
    - Controls compensatoris per les vulnerabilitats que no poden ser resoltes de forma directa.

- Detecció i protecció:

  - Donar suport a l'operació de les eines de ciberseguretat del lloc de treball seguint les indicacions de l'Oficina de QA de Ciberseguretat i de l'Agència de Ciberseguretat (SCCM, MDM, EDR, antivirus).
  - Donar accés a l'Agència de Ciberseguretat i a l'Oficina QA de ciberseguretat a les consoles de gestió centralitzada (SCCM o equivalent), MDM (gestió de dispositius), entre altres, que facilitin la detecció, protecció i actuació en front d'amenaces de ciberseguretat.

- Desplegar dels serveis de diagnosi de la seguretat (anàlisi), protecció i reacció de l'Agència de Ciberseguretat.
- Qualsevol incident de seguretat haurà de ser reportat a l'Agència de Ciberseguretat i a l'Oficina de QA de Ciberseguretat, seguint els procediments de gestió d'incidents establerts per l'Agència de Ciberseguretat.
- L'empresa adjudicatària haurà de facilitar tota la informació i accessos (a les màquines afectades) per facilitar les tasques d'investigació de l'equip de gestió d'amenaces i l'equip de gestió d'incidents de seguretat de l'Agència de Ciberseguretat.
- Subministrar a l'Agència de Ciberseguretat un usuari específic per disposar d'accés a les eines de gestió centralitzada de la configuració dels dispositius (SCCM, WSUS, consoles antivirus, etc.).
- Disposar d'un pla d'actuació davant de ciberatacs validat per la Agència de Ciberseguretat de Catalunya.
- Donar suport de forma immediata per la gestió de qualsevol ciberatac rellevant.
- Integrar-se amb els procediments operatius de gestió d'amenaces de l'agència. En aquest sentit, serà necessari que l'empresa adjudicatària participi de forma activa en les sessions d'orquestració quan sigui requerit per l'Agència de Ciberseguretat.
- Establir conjuntament amb la Oficina de QA de Ciberseguretat pla d'acció per fer front a les principals amenaces aplicables i als vectors d'atacs associats.

- Resposta: Per la correcta gestió de potencials amenaces o d'incidents de seguretat, el proveïdor haurà de:

  - Executar simulacions d'incidents de ciberseguretat coordinadament amb l'Agència de Ciberseguretat, mitjançant la preparació i definició de plans d'actuació en funció del tipus d'amenaça simulat.
  - Detecció i preanàlisi d'incidents materialitzats a través de la recepció, comunicació i triatge inicial de la criticitat.
  - Executar les principals accions de contenció determinades per l'Agència, ja sigui mitjançant eines automàtiques tipus SOAR, o bé accions ad-hoc requerides.
  - Executar les accions d'erradicació i recuperació de tots els punts afectats per l'incident per poder tornar a la normalitat així com la protecció d'un futur impacte.
  - Documentar i mantenir la bitàcola de les accions realitzades durant la gestió de l'incident.
  - Disposar d'una matriu d'escalat 24x7 per la gestió d'incidents de seguretat, així com d'un procediment d'actuació en front ciberatacs.
  - En el cas de gestió de crisis d'incidents de nivell crític o especialment rellevants, l'Agència de Ciberseguretat podrà establir períodes excepcionals que requereixin la generació d'informes d'estat periòdics, així com la presència del responsable de seguretat de l'empresa adjudicatària a les diferents reunions que es puguin realitzar (disponibilitat 24x7).
  - Disposar d'un procediment d'extracció i entrega d'evidències de manera segura (traces, esdeveniments de sistema i/o aplicació, clonat d'actius, etc.) el qual haurà de ser validat per l'Oficina QA de ciberseguretat i l'Agència de Ciberseguretat durant l'inici de la prestació del servei. Aquest procediment haurà de ser executat sempre que l'Agència de Ciberseguretat ho requereixi per la gestió d'incidents de seguretat.
  - Identificar tots aquells actius del servei que no es trobin protegits per un perímetre de seguretat per planificar-ne la seva integració, coordinadament amb l'Oficina QA de ciberseguretat.

- Executar les accions per la identificació, contenció, mitigació o erradicació dins la gestió d'un incident de seguretat indicades per l'Agència de Ciberseguretat dintre del context de la gestió d'incidents.
- Documentar formalment en informes qualsevol activitat realitzada dintre de la gestió d'incidents, els quals podran ser sol·licitats per l'Agència de Ciberseguretat en qualsevol moment. L'Agència de Ciberseguretat es reserva la potestat de poder establir els formats més adients per la generació de la documentació.
- Preservar les evidències segons normativa vigent i amb la qualitat necessària per donar resposta a la informació necessària per la resolució d'un incident de seguretat.
- Quan sigui requerit per l'Agència de Ciberseguretat, l'empresa adjudicatària haurà d'executar les accions de Troubleshooting específiques en l'àmbit de seguretat, amb l'entrega del corresponent informe de finalització.
- Garantir la cadena de custòdia i format de totes les evidències per assegurar la seva validesa jurídica.
- Lliurar a l'Agència de Ciberseguretat tota la informació sol·licitada, garantint el compliment dels següents terminis fixats.
- L'empresa adjudicatària haurà de subministrar els accessos remots necessaris als interlocutors de l'Oficina QA de ciberseguretat i a l'Agència de Ciberseguretat per poder accedir als esmentats agents en cas d'incident de seguretat.
- De forma general, l'empresa adjudicatària haurà de complir amb la norma de gestió d'incidents de seguretat.

Resiliència

Arquitectura, proves de recuperació de desastres i proves de recuperació de backups, l'empresa adjudicatària haurà de:

- Disposar d'un pla de continuïtat dels serveis objecte del contracte i executar proves de recuperació, com a mínim, anuals. Prioritzar les proves sobre els entorns més crítics (directoris actius, DNS, controladors VPN afectats que impedeixen la prestació del servei, xarxes LAN que donen servei a volums grans d'usuaris, etc.). Simular diferents tipus d'escenaris: infecció massiva dels equips, denegació de servei, ransomware que encripta els equips, etc.
- Desenvolupar un pla de continuïtat del lloc de treball, en un escenari en el qual no es pugui accedir a les instal·lacions (escenari de pandèmia), i tots els treballadors públics hagin de prestar el servei de forma remota. El servei d'entrega haurà d'estar preparat per fer front a aquest escenari i assegurar que coneix les actuacions a fer per garantir que el servei el presta amb normalitat i els usuaris poden teletreballar amb unes condicions adequades. Es farà una prova anual amb un grup reduït d'usuaris per comprovar-ne l'efectivitat i coneixement.
- Executar proves de recuperació de backups de cada tipologia, com a mínim semestralment.
- Fer proves de recuperació d'equips (per exemple, recuperar un directori actiu, un servidor d'impressió tipus) així com proves de recuperació de dades (per exemple, recuperar el backup aleatori de l'eina de backup utilitzada).
- Lliurar a l'Agència de Ciberseguretat una planificació del servei, així com els informes i evidències que demostren l'execució de les proves realitzades.

Control d'accessos

L'empresa adjudicatària haurà de complir la norma de control d'accés i la guia de gestió de Comptes d'administració de la Generalitat de Catalunya. L'empresa adjudicatària haurà de:

- Desplegar una solució de doble factor d'autenticació (MFA) per tots els administradors del servei, seguint les directrius de l'Agència.
- Tots els equips dels administradors hauran de tenir instal·lada la maqueta base que estableixi l'Agència de Ciberseguretat, amb les eines de monitoratge i control que l'Agència estipuli. S'acordaran amb l'Agència altres eines addicionals que el proveïdor pugui necessitar per prestar el servei. En cap cas es farà ús d'equips que la Generalitat no hagi autoritzat.
- En cas d'accés remot, tots els administradors hauran d'accedir a través de la solució de VPN corporativa i disposar d'un segon factor d'autenticació (MFA) per minimitzar el risc de robatori de credencials. Igualment, si les eines corporatives ho permeten, qualsevol accés d'un administrador des de dins de la xarxa corporativa, també haurà de disposar d'un doble factor d'autenticació.
- Els equips dels administradors del servei hauran de complir amb els requeriments que fixi l'Agència de Ciberseguretat (maqueta corporativa per administradors), i desplegar en aquests les solucions d'EDR, antivirus, filtratge de navegació i les que l'Agència de Ciberseguretat estableixi, per poder accedir a la xarxa de la Generalitat.
- Disposar d'una plataforma de gestió de privilegis d'administradors (PAM) que garanteixi la identificació única dels administradors, en limiti els seus permisos i permeti gestionar els perfils assignats a cada identificador. Tota l'activitat dels administradors haurà de quedar registrada en el repositori de traces i disponible per l'Agència de Ciberseguretat en tot moment. S'haurà d'establir, coordinadament amb l'Agència de Ciberseguretat, una gestió d'alertes vinculades a aquesta tipologia d'usuaris (per exemple, notificació per correu electrònic de determinades casuístiques de violació de polítiques de seguretat).
- Caldrà limitar al màxim els usuaris administradors locals. Sempre s'haurà de fer amb comptes nominals dels administradors de la xarxa de lloc de treball. En cas de requerir un usuari administrador local, aquest fet s'haurà de notificar a l'Agència per la seva autorització i avaluació del risc associat.
- Validar els usuaris administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades.

Seguretat física

Seguretat de les dependències des de les quals es presta el servei:

- L'empresa adjudicatària aplicarà les mesures de prevenció i protecció d'acord amb els estàndards de la Generalitat de Catalunya en les dependències des de les quals es presta el servei.
- L'empresa adjudicatària vetllarà pel compliment dels estàndards de la Generalitat de Catalunya i podrà ser auditada de forma anual per valorar el grau de compliment i identificar riscos de seguretat.

Formació i conscienciació

L'empresa adjudicatària rebrà formació específica en seguretat per tal de garantir que, en el marc del suport als usuaris, se'ls traslladen directrius adients en matèria de seguretat (la importància d'usar contrasenyes robustes, el bloqueig automàtic dels dispositius per inactivitat, ús del xifrat en les comunicacions, prudència quan es reben correus d'origen desconegut, etc.).

La empresa adjudicatària proveirà del material de formació en seguretat als usuaris, que l'Agència de Ciberseguretat posarà a la seva disposició, com ara: guies ràpides, vídeos demostratius, píndoles formatives, etc.

Aquesta tasca esdevé essencial per conscienciar als usuaris sobre un bon ús dels dispositius de l'entorn de treball i el compliment del marc normatiu aplicable.

Seguiment del servei

L'empresa adjudicatària haurà de reportar mensualment tots els aspectes relacionats amb la ciberseguretat (estat incidents de seguretat, grau de desplegament dels controls de seguretat, indicadors, mètriques, etc.). El format detallat dels informes es pactarà entre l'Institut i l'empresa adjudicatària durant la fase de planificació inicial, tot i que aquests formats podran ser modificats si l'Agència així ho requereix.

Alguns dels informes i actuacions que l'empresa adjudicatària haurà de lliurar són:

- El proveïdor haurà de planificar i conduir dues reunions anuals de seguiment estratègic en matèria de ciberseguretat, adreçades a l'equip tècnic del CPD.
- Aquestes sessions, liderades pel proveïdor en qualitat d'expert, tindran per objectiu:
    - Analitzar incidències rellevants i la seva gestió.
    - Identificar lliçons apreses.
    - Detectar nous riscos o vulnerabilitats emergents.
    - Proposar mesures de millora preventiva i evolutiva.
- Les reunions es podran dur a terme de forma presencial o telemàtica, i tindran una durada màxima de 2 hores cadascuna.