PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE PRESTACIÓ DELS SERVEIS DE MANTENIMENT DE LES INFRASTRUCTURES TIC DEL CONSORCI INSTITUT RAMON LLULL

INDEX

1 OBJECTE DEL CONTRACTE

L'objecte d'aquest contracte és la prestació dels serveis de manteniment de les infraestructures TIC del Consorci de l'Institut Ramon Llull, concretament:

- Servei frontal d'atenció als usuaris
- Servei especialitzat i específic de gestió d'usuaris VIPs
- Servei de suport presencial
- Servei de gestió i operació de dispositius, xarxa local, eines i plataformes
- Servei de coordinació i millora continua
- Servei de suport al desplegament de projectes
- Servei de gestió del coneixement i suport a la gestió del canvi
- Serveis de qualitat i auditoria del servei
- Servei de seguretat.

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

2 NECESSITAT I IDONEÏTAT DEL CONTRACTE

El Consorci de l'Institut Ramon Llull (en endavant, 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, que té com a finalitat la projecció i difusió exterior de la llengua i la cultura catalanes en totes les seves expressions. Per al compliment dels seus objectius, l'Institut dona suport a les polítiques de relacions exteriors en l'àmbit cultural de les institucions consorciades.

Per tal d'acomplir aquesta finalitat, l'Institut té una plantilla prevista per l'any 2024 de 91 treballadors, distribuïts majoritàriament a la seu de Barcelona, amb efectius a l'exterior i personal desplaçat pel programa de residències Faber.

Per dur a terme les tasques corresponents dels diferents usuaris, així com per les necessitats de comunicació interna i externa, és indispensable utilitzar equipaments i sistemes informàtics, els quals requereixen, de forma permanent, d'un servei de manteniment i de suport. Per aquest motiu, l'Institut està interessat en contractar un servei de manteniment de les seves infraestructures TIC. L'adjudicació d'aquest contracte mitjançant un procediment obert és la manera idònia de satisfer aquesta necessitat, i al mateix temps busca promoure l'evolució de l'actual model del servei informàtic cap a un de més eficient i alineat amb l'entorn corporatiu de la Generalitat de Catalunya que faciliti a l'Institut l'adopció de les tecnologies que en cada moment

siguin necessàries per la transformació digital de la gestió de les seves activitats i de la seva imatge institucional.

A continuació es presenta breument l'abast dels principals canvis a realitzar en el servei de gestió de les infraestructures de l'Institut per donar suport a aquesta evolució digital.

Situació Actual del Model de Servei

La situació actual del model dels serveis TIC està caracteritzada per certs aspectes que afecten la seva eficiència, dels quals es destacarien els següents:

- Comunicació Informal i manca de registres: La presència física del personal contractat ha creat una dinàmica d'interacció informal amb el servei tècnic, amb poca documentació i manca de registre de les sol·licituds i incidències. Això pot resultar en una manca de traçabilitat i dificultat per avaluar l'eficàcia de les respostes a les necessitats de l'organització i, sobre tot, a la impossibilitat de detectar a temps accions de millora per la reducció d'aquestes incidències.
- Manca d'Instruccions operatives: L'absència d'un conjunt clar d'instruccions operatives dificulta una gestió eficaç i coherent dels recursos i serveis TIC. Aquesta manca de guies i procediments estandarditzats pot influir en la consistència de les respostes a les sol·licituds i incidències.
- Limitacions en el coneixement del personal contractat: Tot i comptar amb personal especialitzat que es troba físicament a les nostres instal·lacions, existeixen restriccions en els seus coneixements que estan relacionades amb la complexitat i l'abast de les infraestructures que s'han de gestionar. Això pot provocar que, tot i tenir una atenció ràpida per part d'aquest personal, els temps de resolució s'allarguin més del previst.

Cal destacar que aquesta situació no es un focus de insatisfacció del servei actual, però si que són característiques particulars que limiten la seva monitorització i evolució.

Particularitats fonamentals del nou model a desplegar

Amb la finalitat de superar aquestes limitacions dels serveis TIC de l'institut, es necessita desplegar un nou model fonamentat en els següents principis:

- Potenciació de la resolució en primera instància: Es promourà la resolució de les incidències en primera instància des del **Servei d'Atenció a Usuaris** (SAU-IRL), en primer nivell o segon nivell especialitzat, garantint una resposta ràpida i efectiva.
- Registrar tota l'activitat: Tota incidència o sol·licitud serà registrada a través d'una eina pròpia de l'Institut, permetent un seguiment precís i eficient de cada cas i, veient les particularitats d'aquesta activitat, l'estandardització de les solucions a proveir i una guia per l'usuari.
- Indicadors d'Activitat (KPIs) i Nivells de Servei (ANS): S'establiran indicadors clars per avaluar l'activitat del servei, així com els nivells de servei acordats per garantir la satisfacció d'usuaris i eficiència del servei, i que permetin analitzar l'evolució de l'activitat tant en cicles temporals com per unitats de negoci.

- A més, cal que els serveis prestats es recolzin de manera pràctica i contrastable en bones pràctiques com les definides a [1]ITIL o marcs de referencia similars, considerant dins d'aquests marcs de referencia:
    - Les propostes de millora continua, tant en els serveis com de les seves infraestructures
    - L'aplicació de les normes i eines de seguretat TIC definides per la Generalitat de Catalunya a través de la seva Agencia de Ciberseguretat
    - El control de la configuració i el manteniment al dia de la CMDB[2]
    - El suport a la gestió del canvi dels nous processos a desplegar

  Amb aquesta evolució del model de servei TIC de l'IRL, es vol assolir un alineament amb l'entorn corporatiu de la Generalitat de Catalunya, així com amb models estàndards del sector, com són els desplegats pel Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

3 TERMINI DE PRESTACIÓ DEL SERVEI

La prestació efectiva del servei anirà des de l'1 de gener de 2024 (o des de la data de signatura del contracte, si aquesta fos posterior) fins al 31 de desembre de 2024.

Si la signatura del contracte és posterior a l'1 de gener de 2024, es facturaran els dies de serveis efectivament prestats.

Possibilitat de pròrrogues i termini:

Es preveuen quatre pròrrogues de 2 mesos cadascuna a partir de l'1 de gener de 2025, fins a la data màxima del 31 d'agost de 2025.

4 CONTINGUTS DEL SERVEI

A continuació es detallen les activitats a contemplar en cadascun dels serveis a prestar per l'empresa adjudicatària :

4.1 Servei d'Atenció als usuaris

El servei frontal d'atenció a l'usuari/a (SAU), **que s'haurà de prestar en català**, té com a missió atendre totes les sol·licituds dels usuaris i vetllar per la resolució de les mateixes al més aviat possible en horari 12x5 sobre qualsevol infraestructura TIC que facin servir. Aquest servei, com a nivell 1 d'atenció als usuaris, té com a objectius: atendre, enregistrar, diagnosticar **i resoldre**

[1] Information Technology Infrastructure Library

[2] La CMDB (Configuration Management DataBase) és el sistema que permet registrar la informació de la infraestructura i gestió del servei mitjançant entitats anomenades CIs

el màxim de sol·licituds en la primera interacció. **amb** els usuaris; també ha de fer el seu seguiment, informant l'usuari/a de l'evolució i validant amb ell/a la resolució de totes les sol·licituds que s'adrecin via els canals de contacte que s'estableixin.

Funcions:

- Acompanyament i suport a l'usuari/a en la utilització de tots els serveis TIC de l'Institut.
- Acompanyament a l'usuari/a en la realització de peticions i si cal fer la tramitació d'aquestes.
- Registrar qualsevol sol·licitud o comunicació que l'usuari/a no hagi pogut fer en les eines de gestió que l'Institut posarà a la seva disposició. S'haurà d'informar a l'usuari/a del seu número de registre i s'ha de mantenir la informació actualitzada en cada una de les fases i estats de la gestió del tiquet fins al seu tancament definitiu.
- Realitzar les tasques del registre de cada tiquet, de la diagnosi, de la seva resolució i en cas de no ser possible, fer la seva assignació a nivells superiors fent el posterior seguiment de la seva evolució, validant amb l'usuari/a la correcta resolució i per tant el seu tancament.
- Per a l'anàlisi i la resolució tècnica s'haurà de fer servir un seguit d'eines de gestió, com per exemple, l'accés a l'inventari dels usuaris, la seva identificació i accés als seus dispositius remotament per poder resoldre les incidències sense desplaçament sempre que es pugui. L'objectiu és anar augmentant el nivell de resolució en primera interacció. En cas que no es pugui resoldre, o bé perquè no es disposen de procediments a aplicar o perquè la solució aplicada no ha funcionat, ha d'escalar les sol·licituds al nivell de suport que pertoqui, al suport presencial o a grups d'experts dins del mateix servei, o si s'escau, a altres proveïdors involucrats.
- Coordinar extrem a extrem la resolució de totes les sol·licituds. Seguiment de l'evolució de les sol·licituds per mantenir informat a l'usuari/a final de la seva evolució i previsió de finalització
- Seguiment de les sol·licituds que no hagin estat resoltes en el primer contacte per mantenir informat a l'usuari/a final de la seva evolució i previsió de finalització. En el cas de derivar les sol·licituds a altres proveïdors, haurà de fer el seguiment d'aquestes, dels temps de resposta fins a la seva resolució i validar el correcte tancament.
- Amb l'objectiu de maximitzar la resolució d'incidències dels usuaris quan aquests estan en contacte telefònic amb el SAU, però aquest suport frontal no disposa del coneixement o eines per resoldre-ho, l'empresa adjudicatària posarà a disposició d'aquest suport frontal eines *(hot transfer*, eines de col·laboració com el Teams, etc.) perquè, mantenint a l'usuari/a al telèfon o mitjançant transferència a un equip diferent del servei (per exemple tècnics de suport presencial), la incidència es resolgui durant la trucada.
- Suport en l'ús de l'equipament TIC i audiovisual en sales de reunions, sales de premsa, auditoris, aules de formació dels edificis. Resoldrà incidències, dubtes i configuracions d'aquests espais.
- Col·laborar en la gestió de l'inventari dels elements de la CMDB segons les responsabilitats definides, facilitant totes les dades sol·licitades. En cas de detecció d'errors d'inventari dels elements del servei, caldrà gestionar-ho per tal que es corregeixi.
- Escalar al Servei de Coordinació (detallat més endavant) les queixes reportades per l'usuari/a relacionades amb el servei prestat de qualsevol dels proveïdors involucrats.
- Detectar millores en l'autoresolució de l'usuari, i en la documentació de la gestió del coneixement.

- Detectar incidències repetitives per tal d'analitzar el seu possible tractament com a problemes.
- Comunicar, de forma proactiva o reactiva, als usuaris informant d'interrupcions o degradacions de serveis planificats o sobrevinguts.

És important que la gestió remota estigui establerta com a procés de millora contínua perquè d'ella depèn directament el grau de resolució en primera interacció que pot aplicar el servei de suport i, per tant, l'increment de satisfacció del servei per part dels usuaris. En la gestió remota de dispositius, **la manipulació de l'entorn de treball no es pot realitzar sense consentiment de l'usuari/a i en els casos de màxima seguretat amb la presència de l'usuari**. L'Institut, conjuntament amb l'adjudicatari, determinarà quin serà el procediment adequat.

4.2 Servei especialitzat i específic de gestió d'usuaris VIPs i de serveis crítics (GCV)

L'objectiu d'aquest servei és garantir el correcte cicle de vida dels tiquets de les incidències catalogades com a crítiques per al negoci (veure annex I.D Nivells de Servei), així com les sol·licituds d'usuaris identificats com a VIPs. En detectar una sol·licitud d'aquesta tipologia el SAU la traslladarà a un equip de l'empresa adjudicatària que serà qui lideri la seva gestió fins a la resolució. Aquest equip estarà format per tècnics amb un gran coneixement i especialització en cadascun de les infraestructures de l'Institut, sobre tot pel que fa a dispositius individuals i la seva configuració tant des del punt de vista funcional com de seguretat.

Aquest grup s'anomena GCV, Grup de Crítics i VIPs, i si és considera necessari, disposarà d'una bústia única de correu electrònic i d'un telèfon propi solament disponible per aquest col·lectiu. Serà un servei amb disponibilitat de 24x7.

Aquest servei es prestarà amb els recursos del servei continu dimensionat correctament per tal de poder assolir les funcions assignades següents:.

- Realitzar el seguiment extrem a extrem de totes les sol·licituds d'usuaris VIPs i de les incidències definides com a crítiques per l'Institut, per tal de garantir el correcte tractament en forma i temps dels tiquets assignats.
- Donar resposta a aquelles sol·licituds de servei que per la seva especial necessitat requereixin un tractament diferenciat, com poden ser serveis estacionals que són importants en períodes determinats o necessitats urgents per part de l'Institut, adequant els canals de comunicació i els temps de seguiment a les necessitats específiques amb un alt grau de coneixement de l'activitat de l'Institut, per garantir la màxima qualitat en el tractament dels tiquets identificats.
- El GCV garanteix l'estabilitat operativa del servei que presta el SAU, actuant sempre dins d'un marc definit i evitant que aquestes incidències interfereixin en el servei del SAU descrit en el capítol anterior.

4.3 Servei de suport presencial

L'objectiu principal dels serveis de suport presencial és atendre les sol·licituds que no s'hagin pogut resoldre en el suport d'atenció a l' usuari i/o requereixen la presència d'un tècnic.

Aquests serveis són aquells que es troben més propers a l'usuari/a i necessiten realitzar una actuació física davant del seu equipament, o s'ha d'actuar en alguna infraestructura TIC de l'edifici de forma presencial.

És un nivell expert de suport presencial als usuaris i per les infraestructures TIC de l'Institut, que s'encarrega d'assegurar la seva operativitat mitjançant desplaçament al lloc de l'usuari.

Aquest servei es podrà prestar amb tècnics de suport dedicats i per tècnics de suport amb mobilitat territorial quan així es requereixi, i formaran part del servei continu, dimensionat correctament per tal de poder assolir les funcions assignades.

L'empresa adjudicatària posarà a disposició dels seus tècnics eines de comunicació i interacció que permetin que en casos puntuals el servei de suport presencial pugui interactuar online amb l'equip del servei d'atenció frontal (per donar-li suport mentre es manté a l'usuari/a en línia) o d'altres equips experts del servei o, fins i tot, amb l'usuari/a directament per aconseguir una reducció en els temps de resolució (reducció de les interaccions amb l'usuari/a i els temps d'espera).

El servei de suport presencial també disposarà de l'opció de sol·licitar-se sota demanda per donar cobertura a actuacions especials motivades per necessitats de l'Institut.

Funcions:

- Diagnosticar i resoldre les incidències del maquinari i el programari de l'entorn de treball dels usuaris que requereixin intervenció local, a petició dels equips de suport remot. I de la mateixa manera, per les incidències de connectivitat de la infraestructura i electrònica de xarxa d'àrea local que facilita l'accés als diferents dispositius de l'entorn de lloc de treball a la xarxa.
- Sempre que sigui possible, realitzar el suport funcional i tècnic de les sol·licituds mitjançant la connexió remota a la màquina de l'usuari/a. Es un suport tècnic expert que complementa el suport frontal en la gestió de les sol·licituds dels usuaris per tal de reduir el temps de resolució.
- Realitzar el suport tècnic al desplegament de nous sistemes d'informació d'acord amb les indicacions i la documentació proporcionada pels diferents proveïdors.
- Realitzar el suport a la gestió de canvis: ha d'estar informat de la realització i de l'impacte en el servei dels diferents canvis aplicats a les diferents infraestructures de l'Institut. La raó és que ha de vetllar per mantenir informat a l'usuari/a final de forma eficient i estar alerta per poder detectar possibles incidències derivades d'aquests canvis. És responsabilitat seva garantir la coordinació i comunicació cap a primer nivell i la detecció de possibles incidències relacionades amb la seva execució.
- Col·laborar amb l'institut en gestionar un estoc suficient de tots els elements necessaris dels entorns de treball com per exemple ordinadors, impressores, consumibles d'impressores, telèfons mòbils, tauletes, targetes SIM, llicències d'aplicacions, cables de connexió elèctrics, de xarxa o de dispositius, o qualsevol element necessari per a la correcta prestació del servei. I de la mateixa manera, un estoc de tots els elements de xarxa local, com switches, punts d'accés sense fils Wi-Fi, connectors, etc. Aquest material haurà d'estar disponible per tenir temps de reacció pràcticament immediats. Davant una incidència de qualsevol naturalesa, la

prioritat del suport presencial serà restablir el servei al més aviat possible, fent ús de l'estoc d'equipament disponible.

- Realitzar tasques d'instal·lació i configuració presencial de l'equipament de l'entorn de treball. Així com una breu formació bàsica de funcionament de l'equipament a l'usuari.
- Instal·lació i trasllat d'estacions de treball, instal·lació de pissarres i projectors, instal·lació d'impressores, configuració de mòbils i tauletes, substitució de consumibles d'impressores i altres equipaments, substitució d'equipament avariat, connexió física dels dispositius als punts de xarxa, assignació de cablejat de l'electrònica de xarxa als racks d'edifici i gestionar els armaris de connectivitat, comprovar la connectivitat entre els elements de la xarxa local i wifi. Comprovació del funcionament de la connectivitat WAN de l'edifici.
- Realitzarà actuacions sobre la configuració de programari, instal·lació i/o restauració de maquetes i programari necessari pel negoci que no estigui inclòs en la maqueta, arrencada i aturada d'equips, com servidors i elements de xarxa de les sales tècniques i de la infraestructura TIC de l'edifici.
- Realitzar les tasques de l'inventari dels elements del servei de l'edifici o edificis sota la seva cobertura a l'eina d'inventari de l'Institut. Ha d'alimentar i mantenir actualitzada la CMDB amb tots aquells elements que formin part del servei, assignant els elements de configuració a usuaris o espais dels edificis, incloent el servei de recollida i reciclatge d'equips obsolets. Cal recordar que en el casos de reciclatge s'ha de realitzar un esborrat segur de tots els dispositius que siguin reutilitzats o que es vulguin donar de baixa d'acord al marc normatiu de la Generalitat. En cas de baixa definitiva, cal aplicar els procediments de destrucció segura corporatius així com el lliurament d'un certificat que ho acrediti.
- Realitzar les tasques de l'inventari i documentació específiques de les xarxes d'àrea local dels edificis, incloent-hi a més dels elements del servei, també l'adreçament IP de tots els equipaments i dispositius connectats a la xarxa. Aquest inventari haurà de ser a la CMDB de l'Institut així com a les eines d'inventari específiques per a tal fi (esquemes de xarxa, plànols, fotos, actes, etc.).
- Habilitar zones de treball per nous usuaris que s'incorporin, la configuració inicial i els trasllats dins d'un mateix edifici seran coordinats per l'empresa adjudicatària garantint que l'afectació al servei és mínima i d'acord amb les directrius de la gerència de l'Institut.
- Els tècnics presencials han de deixar, quan connectin un nou dispositiu o facin un trasllat, el lloc de treball de l'usuari/a amb tot connectat correctament i amb tots els cables recollits de la millor manera.
- També s'inclou dins d'aquest servei la revisió i racionalització dels equips de reprografia (impressores, fotocopiadores i escàners), i la gestió dels equips multimèdia.

4.4 Servei de gestió i operació remota de les infraestructures, dispositius, xarxa local, eines i plataformes.

Aquest servei es prestarà amb recursos especialitzats (grup enginyeria TIC) per cadascuna de les tasques descrites i conformaran el 2º i 3er nivell del servei. Donat el reduït volum d'activitat, caldrà que l'adjudicatari disposi d'equips multidisciplinaris/multiclients que realitzin les tasques assignades, tant les planificades com les derivades de les diferents peticions i/o incidències que els hi puguin arribar.

Les funcions a realitzar per l'empresa adjudicatària es recullen en els apartats següents però cal que l'adjudicatari tingui la capacitat per adaptar-se a noves tecnologies i procediments de treball que l'Institut vagi desplegant en el transcurs d'aquest contracte.

4.4.1 Gestió, operació i manteniment d'eines i plataformes del lloc de treball

Dins d'aquest apartat s'emmarquen les activitats associades a les infraestructures del lloc de treball que, per sobre de tasques puntuals, ha de vetllar pel control de configuració de les mateixes, per la seva disponibilitat/rendiment i per la seva seguretat. Les principals tasques són:

- Administrar, operar i explotar totes les plataformes de lloc de treball de l'Institut que siguin necessàries per a la prestació dels serveis TIC assignats. Serà el responsable de totes les accions a realitzar en aquestes plataformes.
- Administrar tots els sistemes i servidors de l'entorn del lloc de treball, tals com: directoris de domini, antivirus, inventari, distribució de programari, gestió de dispositius, servidors d'impressió, virtualització d'estacions de treball, monitoratge, inclosos altres sistemes vinculats a entorn del lloc de treball (com servidors de control horari, servidors de cues, servidors que gestionen altres elements com RFID o QR, cartelleria digital, videowalls). El proveïdor és responsable de construir, implantar i administrar les solucions tecnològiques acordades per desplegar el servei.
- Serà el responsable d'operar el directori o directoris per prestar el servei i gestionar l'assignació i permisos dels usuaris als recursos d'infraestructura de l'entorn de treball, segons els usuaris i els perfils definits en el directori corporatiu.
- Gestionar els dispositius, les seves configuracions, maquetes i distribució de programari necessari amb les plataformes tecnològiques, aquestes han de permetre control i gestió remota fer totes les actuacions sobre els dispositius i el programari instal·lat.
- Preparar procediments i guies d'instal·lació de les maquetes, aplicacions i configuracions.
- Preparar procediments, guies d'actuació i eines automatitzades per al tractament i resolució d'incidències.
- Donar suport i formació a l'usuari/a en l'ús del programari i els serveis, al SAU i al servei presencial.
- Totes les activitats hauran d'estar registrades a l'eina o eines de tiqueting designades per l'institut. Les operatives genèriques o específiques del servei hauran d'estar correctament documentades i actualitzades per l'empresa adjudicatària a l'eina o eines que es defineixin per a la gestió documental, i també es reflectiran els canvis en l'inventari d'equipament a la CMDB.
- Referent a l'enginyeria de l'entorn de treball, haurà de:
    - Participar en el disseny d'arquitectures, eines i models de gestió, tant de serveis tecnològics individuals com d'integracions de serveis TIC a l'Institut.
    - Participar en l'homologació de components i solucions TIC, incloent-hi la recollida de requeriments, definició de bancs de proves i realització de tests i pilots de validació.
    - Participar en la documentació tècnica i de gestió dels serveis i solucions, i mantenir-la puntualment actualitzada.
    - Construir, testejar i mantenir les maquetes de l'entorn de treball i proveir la maqueta base als serveis de provisió de maquinari, optimitzant la utilització dels productes de base, d'ofimàtica i especialitzats mitjançant l'adequació de la tecnologia a les necessitats dels usuaris i dels recursos informàtics distribuïts. Comprovar, configurar

i validar el funcionament dels perifèrics i altres equips connectables a les estacions de treball, com telèfons mòbils, projectors, pissarres, etc.

- Preparar, testejar i validar les aplicacions i actualitzacions per tal que puguin ser lliurades a l'entorn de treball de diferents maneres segons la seva viabilitat (local, distribució d'aplicacions, virtualització d'aplicacions, aplicació remota, aplicació al núvol...). Col·laborar amb els equips de manteniment d'aplicacions per assegurar que es podran executar en l'entorn de treball (versions de programari base, navegador, empaquetables, etc.).
- Realitzar i automatitzar el desplegament de programari i la gestió de configuracions a totes les plataformes, tant d'ordinadors personals com de dispositius mòbils.

4.4.2 Gestió, operació i manteniment dels elements locals de xarxa

Pel que fa a les xarxes locals, l'empresa adjudicatària serà la responsable de la seva gestió i manteniment. Tindrà com a objectiu la gestió integral del conjunt d'infraestructures que conformen xarxes d'àrea local dels edificis definits a l'abast i que permeten la connectivitat local dels diferents dispositius de l'entorn de lloc de treball (racks, cablejats, switches, punts d'accés Wi-Fi, tallafocs, etc.). Les principals tasques són:

- Inclou tant la gestió i configuració dels aparells electrònics de xarxa exposats a l'annex I.C o d'altres que es pugui decidir incorporar, com la gestió de la xarxa d'àrea local (LAN), xarxa d'àrea estesa (WAN), xarxa sense fils (WIFI) i serveis de comunicacions de dades, garantint en tot moment la disponibilitat i seguretat del servei.
- Utilització de totes les eines necessàries per poder prestar el servei (inventari, monitoratge, reporting, desplegament i backups, llicències, manteniments, logs, etc.). L'adjudicatari serà el responsable de garantir que les eines tenen, dins els seu abast, tota la planta gestionada.
- Definició dels procediments de gestió, manteniment i monitoratge tant interns com per tercers.
- L'empresa adjudicatària haurà de mantenir inventariats tots els equipaments d'estoc a les eines del servei.
- Operació i control de la xarxa, incloent-hi totes les funcions de suport operatiu per al correcte funcionament, monitorització del tràfic i disponibilitat dels enllaços.
- Col·laboració i assessorament en tasques d'optimització de la xarxa en aspectes d'eficiència i costos.
- Configuració i establiment de connexions VPN, en el cas que l'usuari/a extern requereixi l'accés a la xarxa interna i als servidors principals de l'Institut.
- L'empresa adjudicatària serà la responsable de gestionar els serveis de DNS, DHCP i AAA locals a les seus on es dona el servei de gestió LAN incloses a l'abast.
- Gestió de la interconnectivitat amb totes les oficines exteriors de l'Institut.
- Crear i mantenir un inventari d'adreçament IP de tots els elements presents a les xarxes locals de cada seu segons les directrius definides per CTTI.
- Implementar la seguretat de l'entorn de treball d'acord amb les polítiques i directrius definides per l'Agència de Ciberseguretat de la Generalitat.
- Gestionar l'obsolescència i la renovació tecnològica del maquinari i del programari, quan s'arribi al final de la seva vida útil o del període de manteniment.
- Garantir la integració de les estacions de treball amb les eines de gestió centralitzada de configuració dels dispositius (SCCM, WSUS, consoles antivirus, etc.).

- Posar els mitjans per assegurar que els equips objecte del contracte no tenen vulnerabilitats i, en cas de tenir-ne, establir els plans d'acció per la seva correcció en els terminis que estableixen els ANS i el marc normatiu de la Generalitat de Catalunya.
- Tots els resultats de les anàlisi de seguretat portats a terme per l'Agència seran bolcats al Portal de Seguretat de l'Agència de Ciberseguretat, des d'on l'empresa adjudicatària en podrà fer el seguiment.
- Serà el responsable de gestionar, planificar i implementar els plans de renovació d'equipament, coordinant les tasques del suport presencial i del servei de provisió.

4.4.3 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 dels equips i gestió de garanties remetent la incidència si s'escau, a l'empresa subministradora.
- 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 magneto...), caldrà actuar per mirar de restablir el subministra 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).

4.4.4 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.

4.5 Servei de coordinació a l'Institut

Aquest servei ha de ser el referent davant dels responsables dels serveis TIC de l'Institut com a màxim responsable de la coordinació i seguiment de l'entrega dels serveis anteriorment detallats, actuant com a interlocutor i proposant millores en els serveis i els processos. Per tal d'entendre la seva funció, es presenten les tasques principals a considerar:

- Responsable de la detecció proactiva/reactiva de problemes en base a l'anàlisi de les incidències tractades per part del nivell 1 (SAU i/o Presencial).
- Responsable de proposar millores en els components del servei, metodologies, eines i solucions que es puguin implementar per tal de millorar-ne l'entrega i percepció del servei a l'usuari/a final.
- Encarregat de liderar, dins l'equip dels serveis objecte d'aquesta contractació, la implementació dels plans de millora, transformació, noves solucions i noves eines, operatives, procediments i gestions que l'Institut posi a la seva disposició per a la gestió del servei.
- Analitzar les dades de volumetries i tendències del tiqueting amb l'objectiu de millorar el servei.
- Realitzar els informes requerits per l'Institut per tal de fer un seguiment efectiu dels serveis descrits anteriorment, incloent els derivats de queixes i/o interrupcions del servei.
- Realitzar propostes d'evolució tecnològica, nous productes, serveis, processos de manera continua orientada a l'usuari. Aquestes propostes incorporaran les darreres tecnologies de cara a afavorir l'autogestió de l'usuari/a al seu entorn de treball.
- Coordinació amb els Responsables de Seguretat de la Informació (RSI) de l'Institut per la mitigació/tractament de riscos de seguretat.
- Coordinació operativa amb l'equip de resposta a incidents i amb el SOC de l'Agència de Ciberseguretat davant incidents o possibles amenaces de ciberseguretat que afectin a l'Institut.
- Lliurament d'evidències a l'Agència de Ciberseguretat per la gestió i investigació d'incidents de seguretat, suport per l'aplicació ràpida de mesures de protecció i contenció davant amenaces o ciberincidents, disposar d'informació vinculada al dispositiu, etc.
- Assegurar que tot el personal de l'adjudicatari que presta serveis a l'Institut passin per un pla de formació i conscienciació en matèria de ciberseguretat, amb especial focus en el marc normatiu de la Generalitat i els procediments operatius que li siguin d'aplicació.

4.6 Servei de gestió del coneixement i gestió del canvi

Aquest servei ha de garantir la qualitat i fomentar la millora continua del servei mitjançant diverses iniciatives, com ara l'elaboració de documentació, o a través del **foment i promoció del coneixement per part dels usuaris,** així com per part del propi equip de l'adjudicatari que participi en la gestió dels serveis TIC de l'Institut.

Aquest servei es prestarà amb els recursos del servei continu dimensionat correctament per tal de poder assolir les funcions assignades següents:

- Gestió documental de les operatives dels serveis gestionat. Responsables d'elaborar i mantenir actualitzada tota la documentació de la gestió del servei, procediments, processos, instruccions operatives i tota aquella documentació necessària per a que tots els nivells de l'entrega de servei treballin de forma coordinada.
- Gestió documental de la informació als usuaris: creació i actualització de la documentació publicada als usuaris segons les directrius de l'Institut. Responsable de la informació de la KMDB3 de l'eina de gestió de serveis TIC i que estarà publicada pels usuaris via el portal autoservei o altres eines de consulta de l'usuari
- Creació i actualització de la informació destinada a la consulta dels usuaris. Es podrà requerir la creació de píndoles informatives i formatives amb formats de vídeos o presentacions de power points o pdf., i sempre amb l'objectiu de millorar els temps de resolució de les sol·licituds dels usuaris i fomentar l'auto resolució.
- Responsables de fomentar i garantir que tota l'entrega de servei treballi amb les eines internes i aquelles que l'Institut posi a la seva disposició i que tots tinguin el coneixement necessari sobre la tecnologia, dispositius, equipaments, eines, processos i altres per garantir l'operació del servei i el suport a l'usuari.
- Amb la doble vessant de gestió del coneixement i gestió del canvi, haurà de participar activament a les sessions d'activació de nous serveis, lliurament de projectes que es posin en producció i qualsevol altre que tingui afectació sobre el servei, ja sigui per canvis en les operatives ja actives o per la posada en marxa de nous serveis i operatives associades a aquests.
- Utilitzant els materials i indicacions de l'Agència de Ciberseguretat, impartir sessions formatives (presencials i virtuals) de ciberseguretat als usuaris i professionals vinculats a l'Institut per assegurar que aquests puguin treballar de forma segura, i ser conscients dels riscos de seguretat als quals estan exposats. Aquest procés serà tant recurrent i puntual per projectes de desplegament de noves solucions de seguretat (per exemple, doble factor d'autenticació, certificats de xifrat del correu, etc.).
- En aquesta línia, responsables de distribuir el material de ciberseguretat elaborat per l'Agencia de Ciberseguretat (píndoles, manuals, vídeos, guies ràpides, etc.) als usuaris de l'Institu utilitzant els canals més adients (intranet de l'Institut, correu, portal de l'Agència de Ciberseguretat, etc.) per garantir un bon ús dels dispositius i de la informació del lloc de treball.

4.7 Serveis de 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

[3] Knowledge Management Data Base

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.
  - Auditoria de xarxa (LAN/WIFI): anàlisi de seguretat de la xarxa LAN o WIFI (configuració, ports oberts, vulnerabilitats, equips de comunicacions, protocols de comunicacions, etc.)
  - Auditoria d'aplicacions de l'entorn del lloc de treball: revisió del grau d'actualització de les aplicacions.

4.8 Servei de 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.E que, conjuntament amb l'Institut, s'acordin com més crítics. Aquesta revisió i ampliació del Pla de Seguretat, es farà amb caràcter trimestral i sempre tenint present el principis de l'annex referit.

Aquest pla de seguretat s'utilitzarà per fer el seguiment de l'evolució del desplegament,t 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[4] 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

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

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'Àgencia 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).
  - 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 Inventari i activitat
- Annex I.B Sistemes operatius i programari
- Annex I.C Equipament del centre de procés de dades (CPD'S)
- Annex I.D ANS dels serveis

S'ha estimat que les hores que es consumiran d'aquests serveis serà equivalent als FTE's (1.750 h/any) següents:

SERVEI	FTEs	Hores Anuals
SAU-IRL	0,34	595
Servei Presencial	1	1750
Servei Gestió Infraestructures	0,49	860
Qualitat / Seguretat	0,17	300

L'empresa adjudicatària assignarà els tècnics necessaris considerant aquests requeriments mínims:

- Pel servei de SAU i Suport Presencial es demana un mínim de dos anys d'experiència en llocs similars, amb bons coneixements en les eines i productes estàndard d'usuari final (Windows, Office, Android, etc...), i amb especial sensibilitat amb el tracte a usuaris.
- Pels serveis de gestió sistemes, xarxes i infraestructures, es demana 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 (Windows Desktop, Windows Server, Exchange Server, Linux Apache, VMWARE, MySQL, TOMCAT i especialment en l'administració de base de dades

ORACLE), així com coneixements amplis de gestió i configuració de xarxes, equips de comunicacions, routers i switchs.

Pel que fa referència al Servei Presencial, i a efectes d'eficiència i qualitat del servei, aquest suport el prestaran els mateixos tècnics durant el temps que duri el contracte. En períodes de vacances, baixes o faltes d'assistència de més d'un dia dels tècnics del servei presencial, l'empresa adjudicatària haurà de substituir-los per personal amb la mateixa qualificació professional i experiència i estarà obligada a comunicar les dades de persona designada a l'Institut.

L'Institut podrà demanar el canvi d'aquests tècnics del servei presencial sobre la base de la qualitat, la productivitat i la relació amb els usuaris, amb un preavís de 15 dies. De la mateixa forma, l'empresa adjudicatària també 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, xarxes i infraestructures s'haurà de desplaçar a la seu de 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 (tant de primer com de segon nivell) 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 SAU i 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
- Servei Presencial (11 mesos/any – Agost inactiu):
  - De Dilluns a Dijous: de 9h a 15h i de 16h a 18h
  - Divendres: de 9h a 15h
  - Aquest servei solament es prestarà a les oficines que l'Institut té a Barcelona. Si calgués algun desplaçament a altres instal·lacions, aquest seria prèviament planificat amb l'adjudicatari d'aquest servei.
- Servei gestió Crítics i Vips (12 mesos/any):
  - Cal tenir capacitat per donar cobertura de 24x7 a usuaris VIP que, tot i que la seva activitat la realitzen principalment a les oficines de Barcelona, també se'ls hi poden presentar incidències TIC a desplaçaments que fan arreu del món.
  - També cal tenir capacitat per incrementar puntualment el servei presencial a les oficines de l'Institut davant d'acumulació d'incidències que afectin a processos crítics d'activitat que es donen cíclicament (grans esdeveniments, generació de

nòmines, tancament convocatòries, etc...). A tall orientatiu, aquests processos venen a ocupar uns 150 dies a l'any.

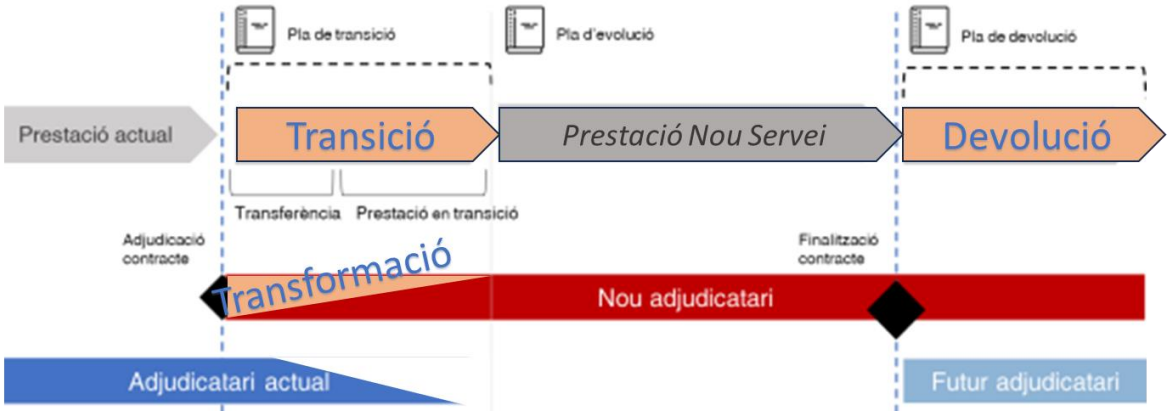
- Per la resta des serveis detallats en aquest plec, en tractar-se de components de gestió i coordinació, no es fixa cap horari concret, però si que cal disponibilitat per desplaçar-se puntualment a les oficines de l'Institut per participar en reunions de seguiment, presentació d'iniciatives de millora, 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 (si hi ha canvi proveïdor)
- 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 seqüencia 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.

Per assegurar una transició fluida i la continuïtat dels serveis, el proveïdor entrant es compromet a contractar els serveis del proveïdor sortint durant la fase de transferència del servei[5]. Aquesta

[5] Cost mensual actual de 7.460 € s/IVA inclòs en import licitació

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:

- Certificat de l'empresa com a partner dels fabricants, HP GOLD PARTNER, APC i MICROSOFT GOLD PARTNER I VMWARE I VEEAMBACKUP, PARTNER LENOVO
- Certificat de l'empresa com a servei tècnic oficial de HP
- Certificació ISO 9001 de qualitat.
- Certificació ISO 14001 gestió mediambiental
- Certificació ISO 20000 Gestió de serveis TIC
- Certificació ISO 27001 relativa als Sistemes de seguretat de la informació
- Certificació dels coneixements i experiència dels tècnics de nivell superior en Windows Desktop, Windows Server, Exchange Server, Linux Apache, VMWARE, MySQL i especialment en l'administració de base de dades ORACLE.

ANNEX I.A – Inventaris i volum activitat

Les volumetries del parc informàtic de l'Institut objecte dels serveis d'aquest plec són les següents:

Portàtils	**120**
Ordinadors	**93**
Monitors	**114**
Impressores	**15**
Escàners	**6**
Videoconferència	**4**
Tablets	**26**

El detall d'aquest parc es presenta en el full excel **Inventari_IRL_2023**

Pel que a les volumetries, i considerant l'activitat del 2023, els volums esperats de tiquets i la seva tipologia seria la següent:

	Mes	Anual
Trucades	160	1.920
Incidències	74	888
Peticions	109	1.308
Consultes	16	192
TOTAL	**359**	**4.308**

ANNEX I.B - SISTEMES OPERATIUS I PROGRAMARI

Sistemes operatius dels servidors:

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

Entorn d'informàtica personal:

- Office 365
- Windows 10 (22H2)
- OpenOffice
- Telefonia IP

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 de control de presència: EVALOSNET
- Programari antispam: GFMAIL
- Eina de monitorització i control d'incidències: KASEYA
- Programari de BBDD: Oracle Sql Server 9i release 2 9.2 i Mysql 5.1.41
- Entorn de desenvolupament: Java/JSP 1.7.0.80 , PHP 5.3.2-1
- Sistema de videoconferència: TANDBERG/ LOGITECH

ANNEX I.C - EQUIPAMENT DEL CENTRE DE PROCÉS DE DADES (CPD'S)

Servidors: 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+

Electrònica de xarxa: Hi ha un total de 11 switchs del model Hp 2920 24 G, i una xarxa wifi amb els dispositius següents:

- Meraki Mr36 (11 dispositius)
- Meraki Mr33 (4 dispositius)

En la part de les comunicacions es disposa dels següents elements:

- Router cisco series 800/2800/2851
- Asa 5516
- 2 Checkpoint

Pel que a les eines desplegades pel proveïdor actual, es destaquen les següents:

- gfi email essentials (seguretat correu/antispam)
- keepit (copia seguretat bústies, onedrive, sharepoint)
- vmware vsphere
- trellix enpoint security
- prey (sistema antirobatori per portàtils i telèfons)
- cisco annyconnect license

ANNEX I.D - 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	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

Eficiència del Servei d'Atenció a Usuaris (SAU):

Codi	Nom de l'Indicador	Valor Objectiu	% Mínim de Compliment	Límit compliment
SAU1	Temps d'espera mitjà	1 minut	90%	<=5'
SAU2	Temps de durada de trucades mitjà	10 minuts	95%	<=30'
SAU3	Número d'incidències/consultes resoltes pel SAU		80%	>=50%

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), accés a xarxa, correu electrònic 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 de 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.E – 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 estabiliran 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, excepcionar 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 y 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 ciber atacs validat per la Agència de Ciberseguretat de Catalunya.
- Donar suport de forma immediata per la gestió de qualsevol ciber atac 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 plan 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 presencia 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 eradicació 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 auditat 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 proveira 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:

- Informe mensual d'estat de ciberseguretat.
- Quadre de comandament de ciberseguretat que inclogui el nivell de ciberseguretat, el nivell de risc i altres indicadors de rellevància.
- Pla d'evolució i innovació en ciberseguretat: que inclogui entre altres aspectes:
  - Proposta i realització d'un simulacre anual de ciberseguretat per avaluar la maduresa del servei en ciberseguretat.
  - La realització de 2 jornades anuals d'innovació en ciberseguretat on s'involucri a l'Agència.
  - La realització de 4 jornades de reflexió anuals on s'analitzin les lliçons apreses, s'identifiquin les principals problemàtiques i reptes en matèria de ciberseguretat.