Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informació

Plec de Prescripcions Tècniques particulars que regeix la contractació del subministrament i implantació de la solució DNS, DHCP, IPAM per l'àmbit Departamental, Intranet i ICS (XR-2018)

Expedient núm.: CTTI-2023-198

Unió Europea
Fons Europeu
de Desenvolupament Regional

CONTINGUT

1. Objecte

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient CTTI-2019-20164 que regeix l'acord marc pels subministraments i projectes de xarxa de la generalitat de Catalunya.

L'objecte de la present licitació és la contractació del subministrament i implementació de l'arquitectura per donar els serveis DNS, DHCP, IPAM i NTP pels usuaris de la Generalitat de Catalunya.

L'objecte del contracte s'emmarca en el:

Lot 2. Xarxes transversals

Es defineix xarxa transversal com el conjunt d'infraestructures i sistemes que permeten la interconnexió i comunicació dels diferents edificis i/o departaments, entre sí i amb serveis remots.

Categories:

- **Servidors centrals.** Equips de processament de dades en format appliance o servidor físic amb virtualització per realitzar les següents funcions de xarxa centrals:
    - Servidors DHCP, DNS, IPAM, NTP
- **Projectes de disseny**
- **Projectes d'execució**

2. Descripció dels subministraments i serveis a realitzar pels adjudicataris

L'abast d'aquest basat contempla els següents serveis a realitzar:

- **Disseny**
- **Subministrament**
- **Implantació**

2.1. Requeriments del disseny proposat

En aquest apartat es definiran els requeriments de l'arquitectura unificada pels serveis DNS, DHCP, IPAM i NTP, a partir d'ara anomenat DDI.

Amb el següent diagrama es defineix quina es l'arquitectura mínima necessària i com s'espera distribuir els serveis en l'arquitectura de la solució.

D'aquesta manera, es podrà revisar amb el adjudicatari el disseny proposat. Fent les modificacions necessaris si s'escau.

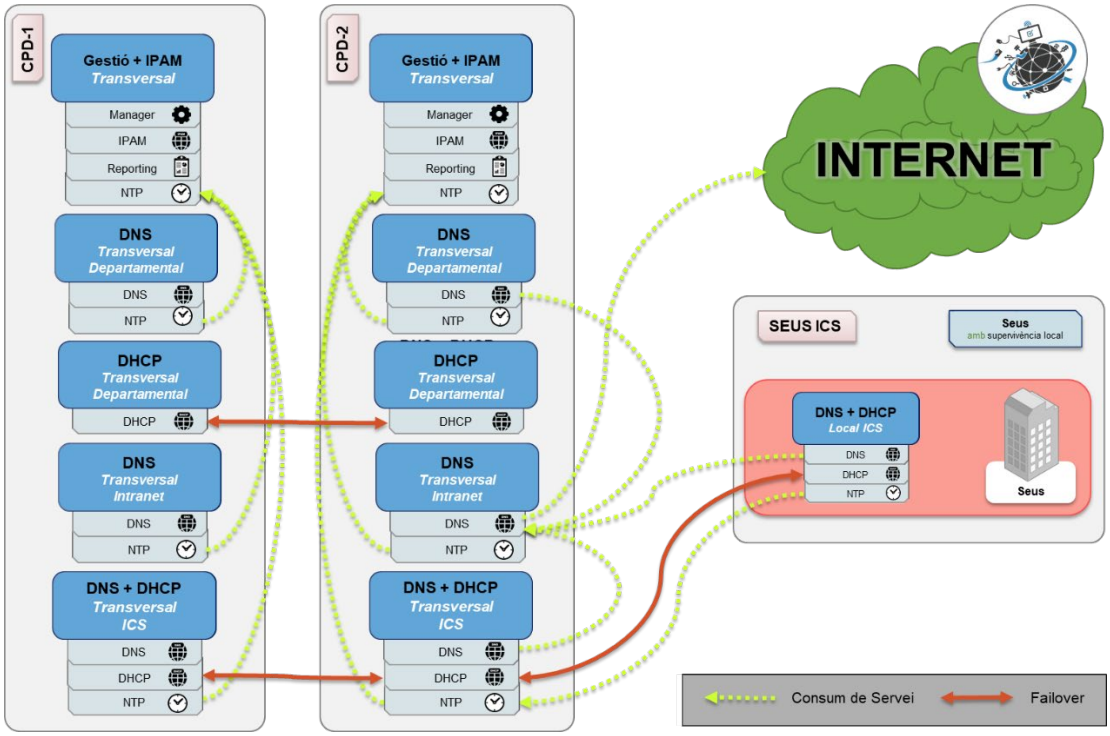


Figura-1 — Diagrama simplificat de l'arquitectura DDI.

Així sorgeixen les següents definicions del disseny:

- Alta disponibilitat en tots els serveis de l'arquitectura DDI.

- Robustesa i resiliència dels components que formen l'arquitectura DDI. Resistència a fallides tenint en compte la capacitat d'adaptació davant de caigudes o degradacions dels diferents components, per tal que no afecti al correcte funcionament de la solució.
- L'arquitectura DDI serà distribuïda en CPDs que decidirà CTTI.
- Gestió centralitzada i delegada per tota l'arquitectura DDI. Basada en Role-Based Access Control.
- Assignació de perfils de gestió amb capacitats granulars mitjançant Rols i Objectes.
- Autenticació a la plataforma mitjançant Radius, Tacacs, LDAP, Directori Actiu i SAML. Preferiblement amb el protocol Tacacs.
- Garantir la capacitat d'integrar la solució DDI amb el sistema de gestió d'identitats i accés a recursos de CTTI (GICAR), mitjançant protocol SAMLv2. Per tal que els administradors puguin accedir amb credencials GICAR.
- Disposició de APIs que permetin desenvolupar automatitzacions de processos amb facilitat. Disposant de documentació, plantilles i exemples que simplifiquin i ajudin en la creació de les automatitzacions.
- Integració amb altres fabricants de forma nadiu, o senzilla amb interfície API RESTful. Aportant llibreries o connectors.
- Garantir la integració amb les eines de monitorització i alertes de CTTI. A més de donar pròpiament en l'arquitectura dissenyada funcionalitats de monitoratge.
- Permetre actualització fragmentada (actualitzacions separades dels blocs definits al plec, per àmbits de servei) de l'arquitectura de la solució. Exposant quin es el màxim temps per l'actualització dels components, que formen els blocs de servei, de l'arquitectura.
- Permetre Rollback (marxa enrere) de qualsevol actualització dels components, que formen els blocs de servei, de l'arquitectura.
- Permetre Backups complets i incrementals, podent-los generar i bolcar de forma àgil i senzilla. Per posteriorment, en cas de ser necessari, poder-los recuperar també de forma àgil i senzilla.
- Enregistrament de tots els successos tant de servei com alertes, per integrar-ho amb eines externes i emmagatzemar-ho.
- <u>Serveis DNS:</u>
  - Servei DNS dedicat transversal per àmbit Departamental de la Generalitat.
  - Servei DNS dedicat transversal per àmbit Intranet de la Generalitat.

- Servei DNS dedicat transversal per àmbit ICS de la Generalitat.
- Serveis DNS dedicats locals per seus amb contingència local per àmbit ICS de la Generalitat.
- Compatibilitat per integrar-se amb la plataforma Microsoft pel servei DNS.
- Compatibilitat per integrar-se amb la plataformes de servei Cloud DNS. Amb el servei DNS On-Prem en mode autoritatiu ocult (master primary) i el servei Cloud DNS com a autoritatiu visible (master slave). Indicant quines solucions Cloud DNS son integrables.
- Possibilitat per integrar-se amb altres plataformes de servei DNS, com Linux.

- Serveis DHCP:
  - Tots els serveis DHCP amb Failover. Que permeti disponibilitat i consistència en el servei en cas de caiguda d'algun servidor.
  - Servei DHCP dedicat transversal per àmbit Departamental de la Generalitat.
  - Servei DHCP dedicat transversal per àmbit ICS de la Generalitat.
  - Serveis DHCP dedicats locals per seus amb contingència local per àmbit ICS de la Generalitat.
  - Compatibilitat per integrar-se amb la plataforma Microsoft pel servei DHCP.
  - Possibilitat de mecanismes per detectar pools DHCP esgotats o prop d'esgotar-se.
  - Possibilitat per integrar-se amb altres plataformes de servei DHCP, com Linux.
- Serveis NTP:
  - Servei NTP global DDI transversal al bloc de servei IPAM. Aquest s'actualitzarà de serveis externs NTP públics.
  - Servei NTP dedicat transversal per àmbit Departamental de la Generalitat. Aquest s'actualitzarà del servei NTP global DDI transversal.
  - Servei NTP dedicat transversal per àmbit Intranet de la Generalitat. Aquest s'actualitzarà del servei NTP global DDI transversal.
  - Servei NTP dedicat transversal per àmbit ICS de la Generalitat. Aquest s'actualitzarà del servei NTP global DDI transversal.

- Serveis NTP dedicats locals per seus amb contingència local per àmbit ICS de la Generalitat. Aquest s'actualitzarà del servei NTP transversal per àmbit ICS.

- Servei IPAM:
  - Servei IPAM transversal i unificat per àmbits Departamental, Intranet i ICS de la Generalitat.
  - Visualització i gestió senzilla dels mapes de xarxa de la Generalitat.
  - Eines de cerca i filtratge de dades.
  - Autodescobriment de xarxes, inspeccionant els equips de la xarxa.
  - Possibilitat per definir diverses vistes per tal de diferenciar els adreçaments.
  - Mecanismes per detectar inconsistències en l'assignació d'adreçaments.
  - Auditoria de Canvis amb històric de 24 mesos.
  - Integració amb SIEM i d'altres eines de recol·lecció de logs. Amb una latència de recepció dels logs que permeti una visualització propera a temps real.
  - Integració amb APIs per aprovisionaments automatitzats.

- Servei Reporting:
  - S'ha de garantir la continuïtat i rendiment de la resta de serveis de l'arquitectura DDI, encara i l'explotació intensiva del servei de Reporting. D'aquesta manera, el servei es pot donar tal com es planteja a la Figura-1, unificat amb el hardware/appliance de Gestió i IPAM, o separat en un hardware/appliance dedicat.
  - Possibilitat de Servei de Reporting en alta disponibilitat.
  - Servei Reporting transversal i unificat pels àmbits Departamental, Intranet i ICS de la Generalitat.
  - Eines de cerca i filtratge de dades i logs.
  - Integració amb SIEM i d'altres eines de recol·lecció de logs (Exemple: SPLUNK). Amb una latència de recepció dels logs que permeti una visualització propera a temps real.
  - Consulta últims 24 mesos
  - El client de reporting ha de permetre la visualització de dades i esdeveniments tan propera al temps real com sigui possible, sense superar els 10 minuts de retard temporal.
  - Visualització a l'eina de reporting. Definint tot seguit els mes destacats:

- Volumetria de peticions recursives,
- Volumetria de peticions autoritatives per zones
- Volumetria, per tipologia, origen i destí d'atacs
- Dominis mes consultats
- Dominis consultats per ip client.
- Dominis en desús/obsolets
- Reports errors (NXDOMAIN, NO DATA..)
- Alarmes d'esdeveniments
- Visualització de tendències

✦ En cas de solució de reporting comporti una integració hibrida amb un servei Cloud, caldrà tenir en compte els següents requeriments:

- Us d'ample de banda limitat. Caldrà que la integració i l'enviament de dades des de l'arquitectura On-Prem cap a la solució de Reporting Cloud utilitzi el mínim d'ample de banda possible. Mitjançant tractament de dades i compressió en l'enviament.
- Seguretat de la connexió de l'arquitectura hibrida. Garantir i maximitzar la seguretat e integritat de les connexions entre l'arquitectura On-Prem i la solució Cloud.
- Alta disponibilitat del servei de Reporting on Cloud.

- Funcionalitats especifiques de seguretat DNS:

✦ DNSSEC. Habilitar la funcionalitat de DNSSEC per tal de validar tota la cadena de confiança en la consulta DNS.

✦ Protecció d'atacs DNS. Capacitat per identificar i evitar els diferents atacs que es puguin rebre en un servei DNS.

- DDoS. Atacs de denegació de servei mitjançant consultes massives DNS malicioses, saturant el servei DNS per tal que no pugui donar resposta a les consultes DNS legitimes.
- DNS cache poisoning. L'atac de DNS cache poisoning és l'acte d'entrar informació falsa a una memòria cache de DNS, de manera que consultes de DNS tornen una resposta incorrecta i els usuaris són adreçats a llocs web incorrectes.
- Atacs de reconeixement i de transferència de zona. Atacs esdevinguts de vulnerabilitats generades per una configuració incompleta o incorrecta del servei, on un atacant pot extreure informació de la infraestructura DNS.

✦ Filtratge DNS. Capacitat per filtrar les comunicacions del servei DNS en funció de les polítiques establertes. Aquestes polítiques de filtratge es poden definir com:

- Custom Lists (Llistes negres i blanques). Una llista blanca (whitelist) o una llista negra (blacklist) de noms, dominis, IPs o CIDRs mitjançant la qual es bloquejarà la resolució DNS.

- Contingut. Es denegaran les resolucions d'aquells registres DNS que estiguin associats als continguts indicats.

- Filtratge RPZ. Habilitar el filtratge de seguretat DNS basat en un estàndard obert i vendor-neutral per l'intercanvi de la informació de configuració dels DNS Firewalls. Mitjançant aquesta informació s'obtenen dinàmicament les llistes de noms, dominis, IPs o CIDRs que es classifiquen com insegurs oferts per fabricants.

✦ Funcionalitats avançades de seguretat DNS. (Threat detection, DNS Inspection)

- Malware. Detecció i bloqueig de resolucions cap a websites i altres servidors que puguin acollir programari maliciós, drive-by downloads/exploits, amenaces mòbils, etc.

- Command and Control Callbacks. Detecció i bloqueig de resolucions, per tal de prevenir la comunicació amb els dispositius compromesos per la infraestructura del atacant.

- Phishing Attack. Detecció i bloqueig de resolucions de websites fraudulentes, que tenen com a objectiu enganyar als usuaris a lliurar informació personal o financera.

- Dominis potencialment perjudicials. Detecció i bloqueig de resolucions de dominis que presenten un comportament sospitós i que poden ser part d'un atac.

- DNS Tunneling VPN. Detecció i bloqueig de resolucions de serveis VPN i possibles encapsulacions de túnels VPN mitjançant la comunicació DNS, que permeten als usuaris disfressar el seu trànsit, podent així evitar les polítiques corporatives.

- Funcionalitats especifiques de seguretat DHCP:

✦ Protecció d'atacs DHCP. Capacitat per identificar i evitar els diferents atacs que es puguin rebre en un servei DHCP.

- DDoS - Starvation attack. Atacs de denegació de servei mitjançant missatges DHCP discover fins que tot el pool d'adreçament IP estigui saturat. D'aquesta manera es satura el servei DHCP legítim amb missatges maliciosos, bloquejant el servei de DHCP legítim.

- DHCP spoofing attacks. Una vegada s'ha completat l'atac de DDoS es pot engegar un servidor rogue DHCP per tal d'enverinar als clients amb informació del router o del servidor DNS servidor del atacant. D'aquesta manera es redirigeix als clients cap un cap a servidors no legítims.

- Security hardening DHCP. Capacitat aplicar polítiques de seguretat a les comunicacions del servei DHCP.

  - DHCP port-level protection. (Polítiques de seguretat per port LAN)

    Es poden utilitzar polítiques de seguretat a nivell de port LAN com a mesura de seguretat en contra dels servidors DHCP no autoritzats. D'aquesta manera, l'administrador de xarxa pot configurar cada port com a confiable o no confiable. Així el port on es connecti o vagi a circular tràfic de DHCP legítim tindrà que habilitar-se com a confiable, i la resta es configuraran com a no confiables bloquejant així tot el tràfic DHCP no legítim.

  - DHCP user-level protection. (Polítiques de seguretat per MAC i/o IP)

    Es permet als administradors del servei DHCP, o dels equips de la xarxa LAN poder controlar l'accés a aquest mitjançant la MAC i/o IP dels dispositius. El filtratge de la capa de connexió permet especificar quines adreces MAC i/o IPs estan permeses a la xarxa i quines tenen denegades l'accés.

- Obtenir i emmagatzemar la traçabilitat dels serveis DNS/DHCP.

  Tenint en compte el consum pels usuaris i dispositius. Com també els períodes de retenció de traces definits en la Norma de Gestió de Traces (NOR0016-C) que defineix un període mínim de 6 mesos online més 12 mesos en repòs, 18 mesos en total.

2.2. Requeriments del Subministrament

En aquest apartat es definiran els punts essencials del subministrament dels components de l'arquitectura unificada pels serveis DNS, DHCP, IPAM i NTP, recollits en els següents punts.

- Tot tenint en compte el diagrama de la Figura-1, es defineixen així els mínims components hardware/appliance, agrupats per blocs de servei, necessaris per desenvolupar l'arquitectura. Podent oferir alternatives a l'arquitectura plantejada.

- L'arquitectura definida haurà de garantir sempre tots els requisits de servei, fins i tot en cas de conviure en un mateix hardware/appliance.

- Tot seguit es defineixen els requisits de hardware/appliance, tenint en compte la Figura-1, agrupant-ho així per serveis en els següents blocs:

  - **Bloc Gestió/IPAM/Reporting Transversal:**

    - Arquitectura:
      - Alta Disponibilitat Datacenter. Dos equips mínim, amb un equip per CPD amb els requeriments indicats.
      - Alta Disponibilitat interfícies 1Gbps (mínim 2 interfícies per equip)
      - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
      - Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

    - Capacitat (per equip):
      - Mes de 3MM Objectes a DDBB. Cada equip ha de suportar un mínim de 3 Milions de objectes en la seva base de dades.
      - Gestió mínima per 32 equips dintre de l'arquitectura definida. (cal incloure totes les llicencies necessàries)
      - Capacitat IPAM per autodescobriment de xarxes per 6000 equips de xarxa. (cal incloure totes les llicencies necessàries)

    - Seguretat:
      - Protecció anti-DDoS. Definim DDoS com atacs de denegació de servei mitjançant consultes massives malicioses, saturant els serveis de Gestio/IPAM/Reporting per tal que no puguin donar resposta a les consultes legitimes. (cal que incloure totes les llicencies necessàries)

  - **Bloc DNS Departamental Transversal:**

    - Arquitectura:
      - Alta Disponibilitat Datacenter. Dos equips mínim, amb un equip per CPD amb els requeriments indicats.
      - Alta Disponibilitat interfícies 1Gbps (mínim 2 interfícies)
      - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
      - Capacitat de publicació d'adreçament Anycast per BGP. Podent respondre a les peticions de servei per les IPs locals pròpies dels appliance i per la IP Anycast, per tal que donar un servei transparent al client en cas de caiguda.

- Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

- Capacitat (per equip):
  - Més de 200K QpS. Cada equip ha de suportar un mínim de 200 mil Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
  - Mes de 3MM Objectes a DDBB. Cada equip ha de suportar un mínim de 3 Milions de objectes en la seva base de dades.

- Seguretat:
  - Domain Name System Security Extensions (DNSSEC). Conjunt d'extensions que afegeixen seguretat al protocol DNS al permetre la validació de les respostes DNS. En concret, DNSSEC proporciona autoritat d'origen, integritat de dades i denegació d'existència autenticada.
    (cal que incloure totes les llicencies necessàries)
  - Protecció d'atacs DNS. Aquesta protecció de seguretat estarà enfocada a atacs al servei DNS [DDoS, DNS cache poisoning, Atacs de reconeixement i de transferència de zona].
    (cal que incloure totes les llicencies necessàries)
  - Filtratge Response Policy Zones (RPZ). Filtratge de seguretat DNS basat en un estàndard obert i vendor-neutral per l'intercanvi de la informació de configuració dels DNS Firewalls.
    (cal que incloure totes les llicencies necessàries)

- **Bloc DHCP Departamental Transversal:**

  - Arquitectura:
    - Alta Disponibilitat Datacenter. Dos equips mínim, amb un equip per CPD amb els requeriments indicats.
    - Alta Disponibilitat interfícies 1Gbps (mínim 2 interfícies)
    - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
    - Capacitat de publicació d'adreçament Anycast per BGP i OSPF
    - Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

  - Capacitat:
    - Mes de 1000 LPs. Cada equip ha de suportar donar un mínim de 1000 Leases DHCP per segon sense arribar a saturar-se ni degradació del servei.

- Mes de 10MM Objectes. Cada equip ha de suportar un mínim de 10 Milions de objectes en la seva base de dades.

- Seguretat:
  - Protecció d'atacs DHCP. Aquesta protecció de seguretat estarà enfocada a atacs al servei DHCP [DDoS - Starvation attack, DHCP spoofing attacks].
    (cal que incloure totes les llicencies necessàries)
  - Security hardening DHCP. Capacitat aplicar polítiques de seguretat a les comunicacions del servei DHCP [DHCP port-level protection, DHCP user-level protection].
    (cal que incloure totes les llicencies necessàries)

- **Bloc DNS Intranet Transversal:**

  - Arquitectura:
    - Alta Disponibilitat Datacenter. Dos equips mínim, amb un equip per CPD amb els requeriments indicats.
    - Alta Disponibilitat interfícies 1Gbps (mínim 2 interficies)
    - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
    - Capacitat de publicació d'adreçament Anycast per BGP. Podent respondre a les peticions de servei per les IPs locals pròpies dels appliance i per la IP Anycast, per tal que donar un servei transparent al client en cas de caiguda.
    - Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

  - Capacitat:
    - Més de 200K QpS. Cada equip ha de suportar un mínim de 200 mil Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
    - Mes de 3MM Objectes a DDBB. Cada equip ha de suportar un mínim de 3 Milions de objectes en la seva base de dades.

  - Seguretat:
    - Domain Name System Security Extensions (DNSSEC). Conjunt d'extensions que afegeixen seguretat al protocol DNS al permetre la validació de les respostes DNS. En concret, DNSSEC proporciona autoritat d'origen, integritat de dades i denegació d'existència autenticada.
      (cal que incloure totes les llicencies necessàries)

- Protecció d'atacs DNS. Aquesta protecció de seguretat estarà enfocada a atacs al servei DNS [DDoS, DNS cache poisoning, Atacs de reconeixement i de transferència de zona].
  (cal que incloure totes les llicencies necessàries)
- Filtratge Response Policy Zones (RPZ). Filtratge de seguretat DNS basat en un estàndard obert i vendor-neutral per l'intercanvi de la informació de configuració dels DNS Firewalls.
  (cal que incloure totes les llicencies necessàries)
- Funcionalitats avançades de seguretat DNS [Threat detection, DNS Inspection – Malware, Command and Control Callbacks, Phishing Attack, Dominis potencialment perjudicials, DNS Tunneling VPN].
  (cal que incloure totes les llicencies necessàries)

- **Bloc DNS/DHCP ICS Transversal:**

  - Arquitectura:
    - Alta Disponibilitat Datacenter. Dos equips mínim, amb un equip per CPD amb els requeriments indicats.
    - Alta Disponibilitat interfícies 1Gbps (mínim 2 interfícies)
    - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
    - Capacitat de publicació d'adreçament Anycast per BGP i OSPF. Podent respondre a les peticions de servei per les IPs locals pròpies dels appliance i per la IP Anycast, per tal que donar un servei transparent al client en cas de caiguda.
    - Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

  - Capacitat (per equip o CPD):

    Les capacitats es podran donar per equip o per CPD, tenint en compte que aquest bloc de servei es trobarà en alta disponibilitat entre CPDs

    - Servei DNS:
      - Més de 100K QpS. Cada equip ha de suportar un mínim de 100 mil Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
    - Servei DHCP:
      - Mes de 500 LPs. Cada equip ha de suportar donar un mínim de 500 Leases DHCP per segon sense arribar a saturar-se ni degradació del servei.

- Seguretat:
  - Servei DNS:
    - Domain Name System Security Extensions (DNSSEC). Conjunt d'extensions que afegeixen seguretat al protocol DNS al permetre la validació de les respostes DNS. En concret, DNSSEC proporciona autoritat d'origen, integritat de dades i denegació d'existència autenticada.
      (cal que incloure totes les llicencies necessàries)
    - Protecció d'atacs DNS. Aquesta protecció de seguretat estarà enfocada a atacs al servei DNS [DDoS, DNS cache poisoning, Atacs de reconeixement i de transferència de zona].
      (cal que incloure totes les llicencies necessàries)
    - Filtratge Response Policy Zones (RPZ). Filtratge de seguretat DNS basat en un estàndard obert i vendor-neutral per l'intercanvi de la informació de configuració dels DNS Firewalls.
      (cal que incloure totes les llicencies necessàries)
    - Funcionalitats avançades de seguretat DNS [Threat detection, DNS Inspection – Malware, Command and Control Callbacks, Phishing Attack, Dominis potencialment perjudicials, DNS Tunneling VPN].
      (cal que incloure totes les llicencies necessàries)
  - Servei DHCP:
    - Protecció d'atacs DHCP. Aquesta protecció de seguretat estarà enfocada a atacs al servei DHCP [DDoS - Starvation attack, DHCP spoofing attacks].
      (cal que incloure totes les llicencies necessàries)
    - Security hardening DHCP. Capacitat aplicar polítiques de seguretat a les comunicacions del servei DHCP [DHCP port-level protection, DHCP user-level protection].
      (cal que incloure totes les llicencies necessàries)

- **Blocs DNS/DHCP ICS Local Seus amb Contingència:**
  Son un total de 8 seus amb contingència local.

  - Arquitectura:
    - Un equip mínim per seu en contingència amb l'arquitectura transversal del ICS, amb els requeriments indicats.
    - Alta Disponibilitat Fonts d'alimentació (per cada equip). En cas de fallida d'una font es pugui mantenir el servei sense degradació.
    - Capacitat de publicació d'adreçament Anycast per BGP i OSPF. Podent respondre a les peticions de servei per les IPs locals

pròpies dels appliance i per la IP Anycast, per tal que donar un servei transparent al client en cas de caiguda.

- Interfície de Gestio Out-of-band (OOB). Tenir un canal de comunicació per la gestió separat del flux de dades habitual. (mínim 1 interfície per equip)

- Capacitat (per equip):

  Les 8 seus amb contingència local, es classifiquen tenint en compte els requeriments de capacitat DNS/DHCP, definint els següents tallatges:

  - ***Mida XL*** (1 seu):
    - Servei DNS:
      - Més de 30K QpS. Cada equip ha de suportar un mínim de 30 mil Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
    - Servei DHCP:
      - Més de 200 LPs. Cada equip ha de suportar donar un mínim de 200 Leases DHCP per segon sense arribar a saturar-se ni degradació del servei.
  - ***Mida M*** (5 seus):
    - Servei DNS:
      - Més de 10K QpS. Cada equip ha de suportar un mínim de 10.000 Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
    - Servei DHCP:
      - Més de 100 LPs. Cada equip ha de suportar donar un mínim de 100 Leases DHCP per segon sense arribar a saturar-se ni degradació del servei.
  - ***Mida S*** (2 seus):
    - Servei DNS:
      - Més de 2K QpS. Cada equip ha de suportar un mínim de 2000 Queries DNS per segon sense arribar a saturar-se ni degradació del servei.
    - Servei DHCP:
      - Més de 20 LPs. Cada equip ha de suportar donar un mínim de 20 Leases DHCP per segon sense arribar a saturar-se ni degradació del servei.

- Seguretat:

- Servei DNS:
  - Domain Name System Security Extensions (DNSSEC). Conjunt d'extensions que afegeixen seguretat al protocol DNS al permetre la validació de les respostes DNS. En concret, DNSSEC proporciona autoritat d'origen, integritat de dades i denegació d'existència autenticada.
    (cal que incloure totes les llicencies necessàries)
  - Protecció d'atacs DNS. Aquesta protecció de seguretat estarà enfocada a atacs al servei DNS [DDoS, DNS cache poisoning, Atacs de reconeixement i de transferència de zona].
    (cal que incloure totes les llicencies necessàries)
  - Filtratge Response Policy Zones (RPZ). Filtratge de seguretat DNS basat en un estàndard obert i vendor-neutral per l'intercanvi de la informació de configuració dels DNS Firewalls.
    (cal que incloure totes les llicencies necessàries)

- Servei DHCP:
  - Protecció d'atacs DHCP. Aquesta protecció de seguretat estarà enfocada a atacs al servei DHCP [DDoS - Starvation attack, DHCP spoofing attacks].
    (cal que incloure totes les llicencies necessàries)
  - Security hardening DHCP. Capacitat aplicar polítiques de seguretat a les comunicacions del servei DHCP [DHCP port-level protection, DHCP user-level protection].
    (cal que incloure totes les llicencies necessàries)

2.2.1. Altres

Tots els equips descrits hauran de complir amb les següents funcionalitats:

- Cal incloure totes les llicències necessàries per tots els requeriments de capacitat i funcionalitats de tots els equips.
- Manteniments a 5 anys a partir de la posada en producció:
  - Es contractarà a nom del CTTI, per tal de facilitar la gestió per tercers.
  - CTTI disposarà de credencials d'accés a les webs de fabricants per:
    - Validar les llicències de suport de fabricant dels equipaments contractats.
    - Seguiment dels casos oberts a fabricant.

- Possibilitat de crear més usuaris per tercers, per poder crear casos directament.
- Subministraments d'actualitzacions de programari durant tot el període de la llicència, incloent totes les releases (minor i major).
- Consultes a fabricant sobre les funcionalitats actuals o futures dels equipaments.

- Tots els tràmits de les gestions d'incidències i/o consultes per aquestes llicències de suport de fabricant, es faran directament amb els fabricant sense que hi hagi intermediaris.
- Gestió de l'escalat i tractament d'incidències tant de programari com de hardware incloent suport online de fabricant durant tot el període de garantia en horari 7x24.
- Enviament i recepció dels equips i/o parts d'equips avariats (RMA) a les ubicacions seleccionades en tot el període de la llicència, en la següent modalitat mínima:
- Modalitat "Next Business day" (NBD): en horari de 8x5.

2.2.2. Quadre resum de subministraments

S'ha realitzat una estimació de l'equipament necessari per donar resposta i suport a l'assegurament de la continuïtat del servei actual.

A continuació es detalla l'estimació de les quantitats necessàries de cada equipament a subministrar durant la durada del contracte:

Bloc de Servei		Quantitats estimades	
Gestió/IPAM/Reporting Transversal		2	
DNS Departamental Transversal		2	
DHCP Departamental Transversal		2	
DNS Intranet Transversal		2	
DNS/DHCP ICS Transversal		2	
DNS/DHCP ICS Local Seus amb Contingència	Mida XL	1	8
	Mida M	5	
	Mida S	2	

2.3. Pla de projecte

En aquest apartat es definiran els punts essencials del projecte per la implantació de l'arquitectura unificada pels serveis DNS, DHCP, IPAM i NTP (DDI).

Les principals tasques que s'hauran de dur a terme són:

- Garantir la qualitat i eficiència de les tasques a realitzar: definició, seguiment i actualització periòdica del pla de projecte, pla de gestió de riscos i pla de qualitat.
- Assistència a totes les reunions necessàries del projecte, per tal de tenir clarament identificada la finalitat del mateix així, com tots el requeriments necessaris.
- Assignació de recursos per projecte.
- Execució de les tasques necessàries per a dur a terme el projecte. L'horari d'execució d'aquestes tasques ha de estar dins de l'horari establert per les mateixes.
- Creació de tota la documentació del projecte, en la que ha d'aparèixer tota la informació referent a aquest (acta d'inici, requeriments, riscos, accions a realitzar, durada, fitxa de tancament, actes de totes les reunions realitzades, etc).
- Reunions periòdiques amb CTTI o les persones que assigni, per fer un seguiment de l'estat de tots els projectes i poder solucionar possibles dubtes / entrebancs.
- Coordinació de tasques amb tercers, si s'escau.
- Creació de nous Procediments i Instruccions Operatives en el cas que fos necessari.
- Creació / modificació de la documentació necessària.

Com ja s'ha comentat anteriorment, tota la documentació referent a cadascun d'aquests projectes haurà d'estar ubicada en servidors del CTTI, tenint aquest accés a la mateixa en tot moment.

Dins les tasques a executar en els projectes cal tenir present:

- Metodologia.
- Disseny de la solució.
- Fases del projecte.
- Fases d'instal·lació i implantació.
- Descripció dels projectes a executar.

2.3.1. Metodologia

Amb l'objectiu de reduir el time to market mantenint els nivells de qualitat exigits pel CTTI, es considera emprar pel control i seguiment de l'estat de projectes la metodologia Scrumban, una combinació dels beneficis de les metodologies Scrum, que posa focus en el treball adaptatiu, la planificació i el resoldre

problemes complexos, amb Lean Kanban, que es centra en reduir els temps d'entrega i la quantitat de treball en curs.

Es complementa amb la metodologia d'execució ESPRIT (Execució i Seguiment de Projectes d'Informàtica i Telecomunicacions) basada en Six Sigma i les millors pràctiques del mercat, que busca:

- Controlar i millorar la gestió dels projectes per assegurar-ne l'èxit.
- Introduir consistència i disciplina a la gestió de projectes en les tres àrees clau d'actuació a l'execució de projectes: Tecnologia, Processos i Persones.
- Assegurar el lideratge efectiu del projecte, garantint la visió, el suport i la implicació de l'alta direcció al projecte. Aquest fet garanteix l'alineació amb les necessitats de negoci.
- Facilitar la gestió per excepció, enfocada a la gestió de riscos.
- Facilitar el coneixement i aprenentatge organitzacional.

Caldrà que l'adjudicatari inclogui els projectes adjudicats a l'eina que disposi en aquell moment el CTTI per fer el seguiment dels projectes. A dia d'avui l'eina disponible és un Panell Kanban.

L'eina de Gestió d'Activitats Kanban facilitarà com a mínim:

- Seguiment global dels projectes tenint en compte els principals paràmetres com per exemple: fites dels projectes, calendari, costos, riscos, etc.
- Identificació dels ítems de treball i fluxos associats.
- Optimització dels fluxos i el rendiment dels equips.
- Seguiment de les polítiques definides.
- Gestió del workflow que asseguri que els ítems associats flueixen i són entregats dins dels nivells de servei definits.
- Gestió de la planificació i calendaris.
- Facilitar el canvi i les activitats de millora contínua.
- Assegurar que les tasques bloquejades segueixin el flux.
- Assegurar que es recullin les mètriques sobre l'efectivitat del sistema.
- Recopilar dades sobre els elements de treball en el taulell Kanban i discutir-los amb el client.
- Assegurar-se que els errors no es repeteixin de forma sistemàtica.
- Trobar mètodes predictius.

El CTTI, per raons de negoci, es reserva el dret de poder modificar, temporal o definitivament, alguns dels aspectes abans descrits, com la documentació a presentar, la priorització dels projectes, etc.

L'adjudicatari s'haurà d'adaptar a les possibles modificacions establertes pel CTTI.

2.3.2. Disseny de la solució

Tenint present els requeriments / necessitats a complir juntament amb el maquinari a adquirir, l'adjudicatari haurà de realitzar un estudi i/o disseny de la solució a implementar.

Per portar a terme aquesta tasca, haurà de reunir-se amb tots els actors necessaris, ja siguin de l'Agència de Ciberseguretat de Catalunya (en endavant ACC), CTTI o aquells que determini CTTI, per aclarir els possibles dubtes i així poder definir la solució.

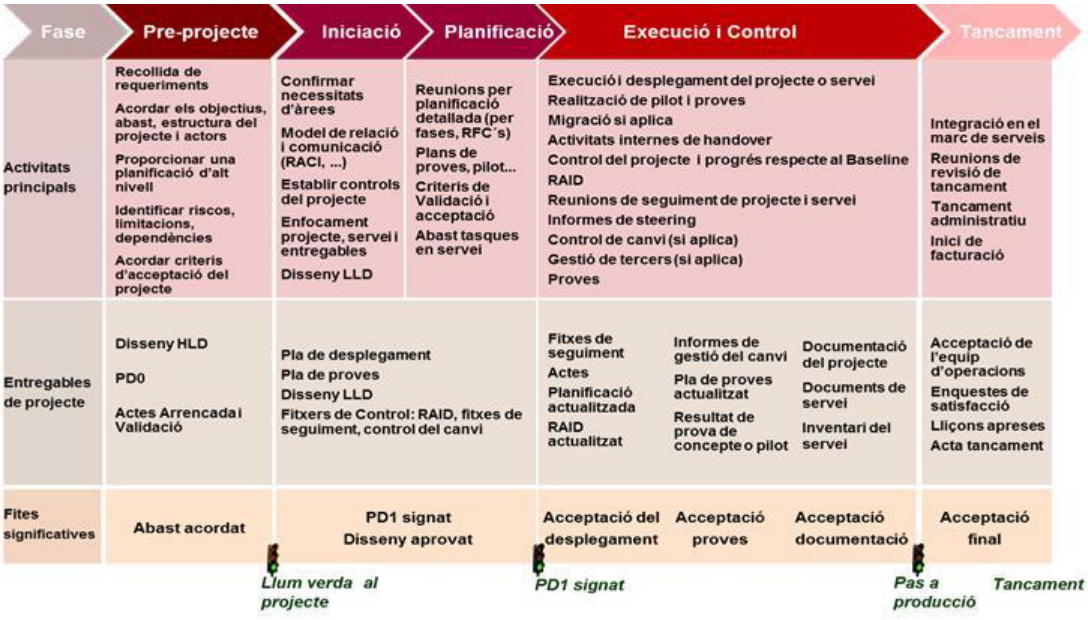
Els entregables mínims d'aquesta fase seran:

- **HLD** (document d'alt nivell) de la solució.
- **LLD** (document de baix nivell) de la solució.

Els documents hauran d'estar validats per CTTI i el seu format, contingut i periodicitat definitius dels documents es pactaran entre l'adjudicatari i el CTTI durant la fase de planificació inicial.

2.3.3. Fases dels projectes

A continuació fem una breu descripció de les diferents fases que composen de forma genèrica un projecte segons la metodologia anteriorment descrita, podent així l'adjudicatari fer-se una idea clara del que els hi pot suposar l'execució dels mateixos.



L'adjudicatari haurà de fer una valoració del projecte que serà compartida amb CTTI i necessitarà l'aprovació d'aquest. Per a cada projecte es determinarà la metodologia / fases a seguir, consensuat en tot moment entre l'adjudicatari i el CTTI.

En cas de conflicte, serà el CTTI qui determini la metodologia / fases a seguir.

En la imatge anterior, es determina els lliurables mínims que ha de tenir cada projecte, podent ser necessària altra documentació addicional per la seva correcta execució.

2.3.3.1. Fase Pre-projecte (Pd0)

En aquesta fase es durà a terme el kick-off del projecte, l'elaboració del Pd0 (document que recull els requeriments tant tècnics com funcionals, es defineix l'abast, els actors implicats, identificació de riscos, dependències, etc.), i validació del mateix.

2.3.3.2. Fase de Planificació (Pd1/HLD)

En aquesta fase es duran a terme el Pd1 (document en el que es desenvolupen i confirmen els punts identificats en el Pd0, i es defineix la proposta de solució tècnica, calendari d'implementació, criteris d'acceptació i validació i anàlisis dels riscos dels projecte), HLD (disseny a Alt Nivell), entre altres. També s'inclou la validació d'ambdós documents.

Es realitzarà el Pla de projecte. Aquest ha d'incloure, entre altres:

- Definició / descripció de totes i cadascuna de les fases per completar el projecte a la seva totalitat.
- Informació necessària per a cadascuna de les fases del mateix, per exemple:
    - Calendari general del projecte.
    - Calendari de totes i cadascuna de les fases i/o subprojectes.
    - Anàlisi de riscos de les diferents fases.
    - Nombre i descripció de RFCs per l'execució de cadascuna de les fases.
    - Pla de proves i validacions per a cada fase.
    - Documentació necessària a entregar al final de cada fase.

2.3.3.3. Fase d'execució

En aquesta fase es duran a terme totes les tasques necessàries per portar a terme el projecte seguint la planificació marcada al Pd1. Es donarà per completada la fase quan s'hagin executat la totalitat de les tasques per entrar en producció, incloent la documentació validada per CTTI, on destaquem les més rellevants:

- Manual d'operació validat.

- Manual d'administració validat.
- Monitorització actualitzada incloent sondes de servei.
- Automatització de les tasques operatives.
- Definició dels informes de Servei.
- Dissenys HLD, LLD finalitzats i validats per CTTI.

L'horari de suport fins que el traspàs a producció quedi finalitzat és de 24x7 (traspàs al proveïdor actual del Nus).

2.3.3.4. Subfase d'instal·lació

El subministrament i instal·lació / configuració de l'equipament que es defineixi com a solució serà una part important del projecte. Aquesta fase inclourà totes les tasques necessàries per a la correcta recepció de l'equipament, la instal·lació del mateix als espais tècnics habilitats, les proves d'acceptació i la posada en marxa de tots els components de la solució que permetin que la xarxa estigui operativa per començar a proveir serveis incloent tots els serveis de monitorització, reporting, gestió, backups i altres possibles necessitats que puguin sorgir, marcades pel CTTI.

Cal considerar una coordinació amb el proveïdor actual del Servei NUS per a la posada en marxa de tots els components i ha de tenir el traspàs de l'explotació dels mateixos a l'actual proveïdor del Servei NUS, incloent-hi, per exemple:

- Dedicació de recursos específics per dur a terme aquest traspàs.
- Generació i entrega de tota la documentació necessària. Aquesta documentació haurà de ser validada pel CTTI prèviament, tant en el seu contingut com en el nombre de documentació necessària (guia operacions, guia administració, monitoratge, HLD, LLD, etc.).
- Document d'acceptació del traspàs.
- L'adjudicatari haurà de tenir molt present, que en el cas de tractar-se de l'ampliació d'un servei que ja s'estigui prestant, no és viable la interrupció del mateix, i en el cas que sigui absolutament necessària s'hauran de buscar les finestres adients per a produir-se.

Aquestes finestres seran establertes pel CTTI en funció de l'impacte i la disponibilitat en el servei. Això inclou qualsevol dia de la setmana i qualsevol hora (cal tenir present que la pràctica totalitat d'intervencions d'aquests entorns es realitzarà en cap de setmana i horari nocturn).

2.3.3.5. Subfase d'implantació

Durant tot el temps que duri la fase d'implantació, l'equip de l'adjudicatari haurà de coordinar-se amb l'actual proveïdor del Servei Nus, per a no interferir en el servei que s'està prestant actualment.

Dins de les tasques a realitzar cal destacar:

- Configuració del nou equipament, basant-se en les configuracions actuals, per així poder seguir prestant com a mínim l'actual servei i no provocar possibles incidències.
- Documentació: A generar per l'adjudicatari tant si es tracta de nova documentació, com de modificar la ja existent. Aquesta documentació, l'adjudicatari l'haurà de definir clarament en totes i cadascuna de les fases que determini per realitzar la totalitat del projecte i haurà d'estar validada pel CTTI. El CTTI es reserva el dret de sol·licitar més informació o un altre tipus. Tota la documentació s'haurà de posar accessible pel CTTI en tot moment. Alguns aspectes que s'hauria de contemplar són:
    - Documentació de servei.
    - Inventaris de xarxa.
    - Inventari de ports.
    - Inventari de VLANs.
    - Inventari d'equipaments.
    - Mapes de servei (físic i lògic).
    - Esquema físic d'ubicació en rack.
    - Documentació de baix nivell dels equips.
    - Manuals d'administració i gestió de tots els equipaments i / o serveis.
        - Reporting de les tasques definides.
        - Creació d'informes periòdics pel control i seguiment de la qualitat, que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, l'eina de seguiment i avaluació del desenvolupament del projecte.
    - La periodicitat dels informes serà definida pel CTTI juntament amb l'adjudicatari. El format exacte i contingut detallat serà proposat per l'adjudicatari i haurà de ser acceptat pel CTTI, que es reserva el dret de fer les modificacions que consideri oportunes.
    - En cas que hi hagi una afectació important al servei caldrà realitzar sessions específiques amb el Centre de Control per tal d'exposar el projecte, clarificar potencials afectacions, determinar els actors implicats i col·laborar en el procés de comunicació de l'afectació del projecte.
    - Transferència de coneixement.
    - El CTTI no assumirà una dedicació significativa de recursos propis o de la Generalitat en les activitats d'implantació i / o posada en marxa.
    - Durant tot el temps que duri la fase d'implantació, l'equip de l'adjudicatari haurà de donar tot el suport necessari al proveïdor actual del Servei Nus a totes les tasques associades a l'administració i operació de la nova infraestructura.

- Durant la fase d'implantació caldrà definir el moment de transferència del servei al proveïdor actual, prèvia validació amb CTTI.

2.3.3.6. Tasques d'instal·lació i implantació

El Pla d'implantació / posada en producció haurà de complir amb els principis i continguts definits i dintre de les tasques a realitzar cal destacar:

- **Peticions a CPD:**

Realització de totes les peticions necessàries d'entrada i sortida d'equipament dels diferents CPDs, realitzar les peticions de reserva d'espai a CPD pels diferents equipaments a instal·lar, realitzar les peticions de cablejat que es requereixin, entre altres.

- **Inventari:**

Proporcionar tota la informació necessària per tal de que els equips quedin inventariats a les eines del CTTI per part del proveïdor actual del Servei Nus. L'adjudicatari haurà de fer la gestió de la provisió de tots els elements necessaris per a la instal·lació i posada en marxa de nous serveis de manera que compleixi els procediments operatius del procés de Gestió de la Configuració i l'inventari per tal d'assegurar el correcte manteniment de la CMDB.

- **Monitorització:**

Definició i creació de les plantilles de monitorització i de les sondes de servei així com la col·laboració en la definició de les alertes de monitoratge, per tal que el proveïdor actual del Servei Nus pugui implementar-ho. El CTTI pot sol·licitar col·laboració puntual a l'adjudicatari per temes específics de monitorització, comprometent-se a col·laborar en tot el que CTTI consideri necessari. Destaquem:

- L'adjudicatari s'haurà d'adaptar al monitoratge que estan realitzant els equips actuals, demanant-li les plantilles i informació necessària al proveïdor del Servei Nus si s'escau. El proveïdor actual del Servei Nus determinarà els requeriments a assolir.
- El proveïdor del Servei Nus serà el responsable de la monitorització dels elements definits. Quan es detecti una alarma es procedirà segons les instruccions operatives definides pels actuals proveïdors.
- El proveïdor del Servei Nus utilitzarà les eines actuals per realitzar les tasques de monitorització, definint tots els llindars d'alertes i el procés operatiu per aquestes, amb la informació que l'adjudicatari els hi proporcioni, i hauran de ser validades tant pel CTTI com pels actuals proveïdors abans que entri en producció.
- En cas que l'equip de monitoratge detecti un comportament anòmal o superació de llindars que suposa un risc de servei o un mal funcionament que pugui afectar als nivells de qualitat es sol·licitarà

a l'adjudicatari d'aquest plec, mitjançant els canals formals definits, la realització d'un estudi per determinar els motius del comportament observat. L'adjudicatari d'aquest plec facilitarà l'informe a CTTI perquè aquest en pugui realitzar la validació, per a fer-ne la seva resolució.

- En qualsevol cas, l'adjudicatari d'aquest plec prestarà la màxima col·laboració als equips de monitoratge per tal de garantir la correcta prestació del servei descrit.
- La resolució de qualsevol alerta, risc detectat abans de l'entrada en producció i/o durant el temps de gràcia un cop estigui en producció serà responsabilitat de l'adjudicatari d'aquest plec, responsabilitat que passarà als actual proveïdors passat el temps abans esmentat.

- **Còpies de seguretat:**

L'adjudicatari haurà de garantir que qualsevol nou equipament entra en el sistema de backups de l'actual servei del NUS. Definició i creació de polítiques de còpies de configuracions amb accés des de l'oficina de seguretat als repositoris de configuracions. L'adjudicatari haurà d'adaptar-se a les eines / polítiques utilitzades per l'actual proveïdor del Servei NUS.

- **Logs:**

L'adjudicatari haurà de garantir que qualsevol nou equipament té configurat el registre de logs. Definició i creació de polítiques de repositori de logs amb accés des de l'oficina de seguretat als repositoris de logs. L'adjudicatari haurà d'adaptar-se a les eines/polítiques utilitzades per l'actual proveïdor del Servei NUS.

- **Accés als equips:**

Accés a tots els equips i creació d'usuaris de lectura i / o escriptura segons aplica, per personal de CTTI, l'oficina de seguretat i / o tercers, amb el suport, si es requereix, de l'actual proveïdor del Servei NUS.

- **Autenticació:**

Autenticació centralitzada i externa a l'equip per la xarxa de gestió contra els servidors d'autenticació de gestió, amb el suport, si es requereix, de l'actual proveïdor del Servei NUS.

- **Pla de proves:**

Un cop instal·lat un equipament i abans d'ésser validat s'hauran de realitzar les proves necessàries a aquests equipaments, des dels llocs sol·licitats i entregar l'informe corresponent, amb el suport, si es requereix, de l'actual proveïdor del Servei NUS. Aquestes proves poden ser, segons apliqui, per exemple:

- Proves de rendiment.
- Proves d'estrès.
- Proves de qualitat.

- Proves de continuïtat.
- Proves de capacitat.
- Proves d'usabilitat.

- **Check-list:**

Definició i creació d'una Check-list validada prèviament per CTTI i per l'oficina de seguretat, per a garantir el correcte funcionament del servei sol·licitat, amb el suport, si es requereix, de l'actual proveïdor del Servei NUS.

- **Reporting:**

Aportar la informació necessària per tal de que el proveïdor del Servei NUS pugui definir i implementar el reporting segons necessitats determinades per CTTI i per l'oficina de seguretat. Aquesta ha de ser accessible a través de les eines actuals del servei NUS.

- **Automatització:**

Aportar tota la informació necessària per tal que, en la mesura del possible, el proveïdor del Servei NUS pugui automatitzar el major nombre de processos com ara, per exemple, el procés de commutació d'un CPD a l'altre.

- **Govern de la dada i mapa de carreteres:**

Proporcionar tota la informació necessària per tal de que el proveïdor del Servei NUS pugui assegurar que continuïn operatius el Govern de la dada i el mapa de carreteres.

- **Documentació:**

Creació de tota la documentació associada (tota la documentació haurà d'ésser validada pel CTTI i per l'oficina de seguretat) i dipositada als repositoris que CTTI indiqui. Destaquem:

- Esquema topològic del servei (físic i lògic) i esquema d'interrelació amb altres elements de la xarxa i amb els elements de protecció.
- Actualització de tots els esquemes existents. Aquesta documentació l'adjudicatari l'haurà de demanar a l'actual proveïdor del Servei NUS i en el cas que no existeix, l'haurà de crear.
- Relació d'equipaments (versions, configuració, funcionalitats disponibles, funcionalitats activades, entre d'altres).
- Documentació associada a les configuracions dels equipaments.
- Manuals d'operació/gestió.
- Contractes vinculats/contractes de suport i manteniment de la solució adquirida.
- Documentació de servei. Per exemple: inventaris de xarxes o ubicació física dels equips.

- **Gestió del canvi:**

El principal objectiu de la Gestió de Canvis és assegurar que, si un canvi es porta a terme, es faci de la manera més eficient, seguint els procediments establerts i garantint en tot moment la qualitat i continuïtat del servei TIC.

Les activitats que es contemplen en la Gestió de Canvis es mostren a la matriu de responsabilitats següent:

Activitats operatives del procés de Gestió de canvis	CTTI	Adjudicatari	SAU	Client
Generació de les instruccions de categorització del canvi	A	R		
Aprovació i Planificació	A,R	R	I	
Implementació	A	R		
Comunicació al client	I	C	A,R	I
Acceptació/Reobertura	I	I	I	A,R
Generació d'Informes	A	R	I	

R= Responsables; A= Aprovador; C=Consultats; I=Informats

Qualsevol canvi haurà de seguir l'operativa establerta a la guia IO Gestió del Canvi del NUS, i per aquesta raó, l'adjudicatari serà el responsable de, principalment:

- Pre-reserva de finestra de RFCs segons normativa CTTI.
- Assistència a CABs (ordinàries) amb el proveïdor del Servei NUS / CTTI / àmbits per defensar els canvis.
- Assistència a ECABS (extraordinàries) amb el proveïdor del Servei NUS / CTTI / àmbits per defensar els canvis.
- Proporcionar la informació al proveïdor del servei NUS per tal que puguin introduir els canvis a Remedy.
- Seguiment del canvi a Remedy.
- Identificació de validadors per a executar el Canvi (Departaments / Proveïdors).
- Interlocució amb el Centre de Control CTTI.
- Enviament de la fitxa del RFC per a tenir-ho recollit dins del Pla d'Acció global.
- Informar dels Canvis al Gestor de Canvis.
- Crear un PPT per a cadascun dels RFC que es vulgui executar.
- Aquest PPT s'haurà d'omplir seguint unes plantilles ja desenvolupades i que es posaran a disposició de l'adjudicatari.
- Informar de l'evolució del RFC i el seu resultat.
- Posar-se en contacte amb el diferents proveïdors i / o clients per a la validació dels RFCs.
- Fer un informe històric de l'execució dels RFCs, on apareguin les dades mes significatives.

L'adjudicatari haurà de tenir molt present, que en el cas de que es dugui a terme l'ampliació d'un servei que ja s'està prestant, no es viable la interrupció del mateix, i en el cas que sigui absolutament necessària s'hauran de buscar les finestres adients per a produir-se. Aquestes finestres seran establertes pel CTTI en funció de l'impacte i la disponibilitat en el servei. Això inclou qualsevol dia de la setmana i qualsevol hora (cal tenir present que la practica totalitat d'intervencions d'aquests entorns es realitzarà en cap de setmana i horari nocturn).

Donada la situació actual, el CTTI es reserva el dret de modificar qualsevol dels punts anteriors.

- **Coordinació:**

L'adjudicatari, d'entre els recursos assignats pel projecte, haurà d'assignar un en concret que assumeixi les següents funcions generals, entre altres:

  - Coordinació amb els responsables de l'oficina de seguretat de les accions a prendre.
  - Assessorament directe a l'oficina de seguretat.
  - Autorització del començament de les fases.
  - Definició i revisió dels objectius del projecte i selecció de la millor alternativa per assolir-los.
  - Comunicació / distribució de la informació concernent a cada grup de treball i col·laboració amb CTTI i amb l'oficina de seguretat en la coordinació i gestió amb els usuaris i / o altres proveïdors en les validacions funcionals i les posades en producció del servei.
  - Assegurar periòdicament el compliment dels objectius totals i parcials del projecte, vigilant i mesurant el progrés del projecte i prenent accions correctives segons es requereixi.
  - Realitzar un control dels riscos que poden afectar al projecte.
  - Formalització de l'acceptació de fases parcials i del projecte en la seva totalitat, garantint un final ordenat i documentat.
  - Coordinació, programació i supervisió de reunions.
  - Supervisió de la documentació del projecte.
  - Coordinació de les presentacions a realitzar del projecte durant el mateix.
  - Suport, col·laboració i coordinació amb proveïdors que gestionen les comunicacions de la Generalitat de Catalunya i d'altres si fos necessari.
  - En el cas de que es tracti d'un nou servei o bé un canvi de proveïdor, cal involucrar al grup corresponent dedicat a Preparar al Servei del CTTI.

2.3.3.7. Fase de tancament

En aquesta fase es revisen els criteris d'acceptació del projecte, es porta a terme el document d'Entrega de Servei i es formalitza el tancament del mateix. Es donarà per finalitzat el projecte un cop validat per CTTI, destacant els següents punts:

- Finalització del procés de CTTI d'entrada en servei.
- Entrada a totes les eines operatives de CTTI (Remedy, inventaris, etc.), per part del proveïdor del Servei NUS amb suport de l'adjudicatari.
- Modificació de la Guia del servei i procediments relacionats per part del proveïdor del Servei NUS amb suport de l'adjudicatari, i validat per CTTI.
- Finalització de les formacions a CTTI i oficines de governança del nou servei.
- Finalització de totes les tasques pendents del projecte.
- Validada la documentació del projecte. Entre altres:
  - Manual d'operació validat.
  - Manual d'administració validat.
  - Monitoratge actualitzat incloent sondes de servei.
  - Informes de servei definit i primer esborrany.
  - Dissenys HLD, LLD finalitzats i validats per CTTI i la resta d'interlocutors implicats.
- Preparació del Document d'Entrega de Servei i la corresponent validació per part del proveïdor Servei NUS i CTTI.

El Document d'Entrega de Servei haurà de contenir com a mínim els següents punts:

- Dades del Projecte:
  - Abast Inicial.
  - Abast real del projecte.
  - Evolució i problemàtiques del projecte.
- Disseny Solució Tècnica:
  - Disseny Inicial.
  - Disseny Final.
- Quadre de Servei:
  - Inventari (Equipament, adreçament, circuits,...).
  - Manteniments / llicències.
  - Instal·lació segons codi bones pràctiques.
  - Actualització esquemes/layouts/descripcions interfícies/fluxes.
  - Autenticacions.
  - Impacte xarxa Seguretat visibilitat.
  - Monitorització.
  - Backups.
  - Logs.
  - Pla de continuïtat / disponibilitat.

  - Pla Operacions.
  - Pla Administració.
  - Pla Capacitat.
  - Pla de proves.
  - Instruccions Operatives.
  - Dissenys HLD / LLD.
  - Guies de Servei.
  - Informes de Servei.
  - Formacions.
  - Neteja configuracions obsoletes.
  - Retirada equipament i cablejat en desús.
  - Automatitzacions.
  - Comunicat de Servei.
- Pla de disponibilitat.
- Pla de capacitat..
- Riscos Mitigats i Detectats
- Punts pendents a tractar fora del projecte.
- Acceptació del Projecte.
- Històric de versions.

2.3.4. Descripció dels projectes

2.3.4.1. Introducció

En l'escenari actual es pot diferenciar dues plataformes a tenir en compte:

- **Grid Departamental**. Proporciona Servei de DNS i DHCP Departamental.

  La plataforma Departamental està formada per 7 nodes principals (2 nodes DNS Departamental, 2 nodes DHCP, 2 nodes spare i 1 node reporting) i 5 nodes 'satèl·lits'. Els nodes principals són els que suporten els serveis de manera global i es troben físicament als datacenters de CTTI. Amb excepció del node de Reporting, la resta de nodes es troben redundats als datacenters de CTTI.

  Els 5 nodes satèl·lits es troben instal·lats a dependències de diferents departaments, oferint un servei DNS de contingència o 'd'últim recurs' en cas que el departament perdés la visibilitat amb els nodes principals.

  Tota la plataforma actual es composa d'equipament del fabricant Infoblox i tots els equips formen part de d'una mateixa plataforma anomenada GRID, que disposa d'una gestió centralitzada. L'equip nuclear del GRID s'anomena GRID MÀSTER, i el seu rol principal es gestionar el GRID i mantenir la base de dades de totes les configuracions de la resta d'equips.

Tota la plataforma actual es gestiona des de una única consola de Gestió. Aquesta consola de gestió la proporciona el node amb el Rol de GRID MASTER i permet:

- Aplicació de gestió.
- Gestió centralitzada, incloent els updates de software i la instal·lació de pegats.
- Rols d'accés.
- Sincronització de les dades de tots els nodes.
- Monitoratge i reporting

La plataforma d'administració conté un IPAM que també es gestiona i s'emmagatzema a la base de dades del GRID MÀSTER. L'IPAM de la plataforma departamental conté informació relativa a les xarxes de WAN, indicant per cada xarxa el Departament, la Seu, l'operador de WAN, data de creació...

- **Grid Corporatiu**. Proporciona Servei de DNS Corporatiu a Intranet, Internet i Salut.

  La plataforma Corporativa està formada per 7 nodes principals (2 nodes DNS Intranet, 2 nodes IPAM, 1 node reporting i 2 nodes DNS Anella Sanitària). Amb excepció del node de Reporting, la resta de nodes es troben redundats als datacenters de CTTI.

  Tota la plataforma actual es composa d'equipament del fabricant Infoblox i tots els equips formen part de d'una mateixa plataforma anomenada GRID, que disposa d'una gestió centralitzada. L'equip nuclear del GRID s'anomena GRID MÀSTER, i el seu rol principal es gestionar el GRID i mantenir la base de dades de totes les configuracions de la resta d'equips.

  Tota la plataforma actual es gestiona des de una única consola de Gestió. Aquesta consola de gestió la proporciona el node amb el Rol de GRID MASTER i permet:

  - Aplicació de gestió.
  - Gestió centralitzada, incloent els updates de software i la instal·lació de pegats.
  - Rols d'accés.
  - Sincronització de les dades de tots els nodes.
  - Monitoratge i reporting

  L'IPAM de la plataforma Corporativa conté informació relativa a totes les xarxes utilitzades al NUS, indicant per cada xarxa el LOT, Bulding Block, CPD, data de creació...

2.3.4.2. Entorn departamental

2.3.4.3. Plataforma de gestió centralitzada

El projecte consistirà en la instal·lació, configuració i posada en servei de la nova plataforma centralitzada transversal (gestió, IPAM, reporting i NTP), incloent l'activació de totes les funcionalitats actuals i les noves funcionalitats que es consideren al plec. Tindrà una durada de 3 mesos.

Entre les tasques a realitzar a banda de les genèriques especificades, el projecte caldrà que inclogui totes les accions necessàries, destacant:

- Definir la nova arquitectura de la solució. Aquests nous dissenys dictaminaran les quantitats d'equipament a adquirir, adequant el maquinari als estàndards d'Alta disponibilitat del NUS i permetent l'administració i operació tant del servei com de la seguretat separades.
- Posada en marxa segons el descrit a les fases del projecte que inclou, entre d'altres:
    - Instal·lació de l'equipament transversal segons el disseny i funcionalitats indicades.
    - Configuració de totes les funcionalitats descrites en l'apartat de l'equipament i migració de totes les funcionalitats actuals per que esdevingui una plataforma de gestió centralitzada.
    - Configuració o creació dels entorns necessaris per a la correcta gestió transversal, com per exemple, IPAM, reporting o NTP.
    - Pla de proves.
    - Integració amb directori corporatiu per la provisió i autenticació automàtica a traves del nostre sistema d'identitat (GICAR).
    - Integració amb les eines de recol·lecció de logs, backup, NTP i de Reporting.
    - Integració amb la Monitorització, Inventari i Reporting del NUS.
    - Integració dels Serveis dintre dels plans de Backups, de Versions (PVER) i de Continuïtat (PCON) del NUS.
    - Posada en producció i transferència de coneixement.
    - Treure l'equip de producció si no presta servei segons el descrit a les fases del projecte.
    - Actualització de la documentació.
    - Creació d'informes de servei.

2.3.4.4. Substitució i migració de la solució DNS-DHCP Departamental

El projecte consistirà en la substitució de la solució de la plataforma Departamental actual segons els requeriments de disseny i funcionalitats indicades. Tindrà una durada de 6 mesos.

Entre les tasques a realitzar a banda de les genèriques especificades, el projecte caldrà que inclogui totes les accions necessàries per a la seva migració, destacant:

- Definir la nova arquitectura de la solució. Aquests nous dissenys dictaminaran les quantitats d'equipament a adquirir, adequant el maquinari als estàndards d'Alta disponibilitat del NUS i permetent l'administració i operació tant del servei com de la seguretat separades.
- Posada en marxa segons el descrit a les fases del projecte que inclou, entre d'altres:
    - Instal·lació de l'equipament DNS i DHCP segons el disseny i funcionalitats indicades.
    - Configuració de totes les funcionalitats descrites en l'apartat de l'equipament i migració de totes les funcionalitats actuals.
    - Pla de migració de les dades actuals a la nova solució, creant els entorns i vistes que siguin necessàries.
    - Integració dins la plataforma de gestió centralitzada (IPAM, reporting, entre altres).
    - Integració amb les eines de recol·lecció de logs, backup i de Reporting.
    - Integració amb la Monitorització, inventari i Reporting del NUS.
    - Integració dels Serveis dintre dels plans de Backups, de Versions (PVER) i de Continuïtat (PCON) del NUS.
    - Integració amb directori corporatiu per la provisió i autenticació automàtica a traves del nostre sistema d'identitat (Gicar).
    - Posada en producció i transferència de coneixement.
    - Treure l'equip de producció si no presta servei segons el descrit a les fases del projecte.
    - Actualització de la documentació.
    - Creació d'informes de servei.

2.3.4.5. Substitució i migració de la solució DNS Intranet

El projecte consistirà en la substitució de la solució de la plataforma Corporativa actual segons els requeriments de disseny i funcionalitats indicades. Tindrà una durada de 6 mesos.

Entre les tasques a realitzar a banda de les genèriques especificades, el projecte caldrà que inclogui totes les accions necessàries per a la seva migració, destacant:

- Definir la nova arquitectura de la solució. Aquests nous dissenys dictaminaran les quantitats d'equipament a adquirir, adequant el maquinari als estàndards d'Alta disponibilitat del NUS i permetent l'administració i operació tant del servei com de la seguretat separades.
- Posada en marxa segons el descrit a les fases del projecte que inclou, entre d'altres:
    - Instal·lació de l'equipament DNS i DHCP segons el disseny i funcionalitats indicades.
    - Configuració de totes les funcionalitats descrites en l'apartat de l'equipament i migració de totes les funcionalitats actuals.
    - Pla de migració de les dades actuals a la nova solució, creant els entorns i vistes que siguin necessàries.
    - Integració dins la plataforma de gestió centralitzada (IPAM, reporting, entre altres).
    - Integració amb les eines de recol·lecció de logs, backup i de Reporting.
    - Integració amb la Monitorització, inventari i Reporting del NUS.
    - Integració dels Serveis dintre dels plans de Backups, de Versions (PVER) i de Continuïtat (PCON) del NUS.
    - Integració amb directori corporatiu per la provisió i autenticació automàtica a traves del nostre sistema d'identitat (Gicar).
    - Posada en producció i transferència de coneixement.
    - Treure l'equip de producció si no presta servei segons el descrit a les fases del projecte.
    - Actualització de la documentació.
    - Creació d'informes de servei.

2.3.4.6. Entorn Salut

2.3.4.7. Posada en servei de l'equipament per a l'entorn de Salut

El projecte consistirà en la posada en servei de l'equipament per proporcionar el servei de DNS/DHCP pel ICS transversal i de forma local segons el descrit a la licitació. Tindrà una durada de 3 mesos.

Entre les tasques a realitzar a banda de les genèriques especificades, el projecte caldrà que inclogui totes les accions necessàries per a la seva instal·lació, destacant:

- Definir la nova arquitectura de la solució. Aquests nous dissenys dictaminaran les quantitats d'equipament a adquirir.
- Posada en marxa segons el descrit a les fases del projecte que inclou, entre d'altres:
  - Instal·lació de l'equipament DNS i DHCP segons el disseny i funcionalitats indicades.
  - Configuració de totes les funcionalitats descrites en l'apartat de l'equipament.
  - Integració dins la plataforma de gestió centralitzada (IPAM, reporting, entre altres).
  - Integració amb les eines de recol·lecció de logs, backup i de Reporting.
  - Integració amb la Monitorització, inventari i Reporting del NUS.
  - Integració dels Serveis dintre dels plans de Backups, de Versions (PVER) i de Continuïtat (PCON) del NUS.
  - Integració amb directori corporatiu per la provisió i autenticació automàtica a través del nostre sistema d'identitat (Gicar).
  - Traspàs de totes les configuracions Legacy.
  - Posada en producció i transferència de coneixement.
  - Creació d'informes de servei.

2.3.4.8. Durada dels projectes

Els projectes definits poden ser executats en paral·lel, tenint en compte les relacions i dependències entre ells.

La durada i planificació estimada és la següent:

	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Subministrament de material												
Gestió centralitzada												
DNS Transversal Departamental												
DNS Transversal Intranet												
DNS Transversal ICS												

3. Condicions d'execució de la solució DDI

3.1. Estructura organitzativa

Dins d'aquest capítol es defineixen els perfils que han de formar l'estructura organitzativa que proposi el licitador, així com de forma il·lustrativa les principals funcions, que no úniques, que han de desenvolupar.

Els recursos humans assignats per l'adjudicatari han de tenir la qualificació necessària per a poder garantir amb èxit la implantació de la solució DDI.

El CTTI es reserva el dret de demanar el canvi d'algun recurs si detecta que no es capaç de complir amb les mínimes exigències que són necessàries. En aquest cas, l'adjudicatari haurà de presentar un pla de canvi del/s recurs/os, que haurà de ser aprovat pel CTTI.

Composició dels punts per facilitar la comprensió de les necessitats demandes:

- Funcions del perfils: Inclou el detall de les responsabilitats que hauran d'assumir els perfils segons les funcions assignades.
- Idoneïtat dels perfils: Inclou les característiques acadèmiques i experiència professional que haurà de complir cada perfil.
- Proposta tècnica i organitzativa: Inclou el detall dels perfils de l'equip tècnic que el licitador consideri més adequat per a la implantació de la solució DDI.

3.1.1. Funcions dels perfils

Les funcions mínimes que hauran d'assumir aquests perfils per a la correcta implantació de la solució són les següents:

- **Responsable de compte:** Aquest perfil correspondrà al responsable màxim (del contracte) de l'adjudicatari enfront del CTTI, vetllant per que aquest es compleixi.

  Principalment és el responsable màxim dels àmbits econòmic, contractuals, organització i estratègia de prestació del servei.

- **Cap de projecte**: Encarregat de planificar les activitats dels serveis de suport i projectes, realitzar anàlisi de desviacions d'abast, cost i temps, gestionar i fer seguiment dels recursos, dels canvis, riscos i coordinar-se amb altres proveïdors. Realitzarà funcions de direcció, planificació, control i supervisió dels serveis i projectes i dels recursos humans assignats a aquests.

  Serà la persona que haurà d'assegurar l'èxit del servei i els projectes dels que serà responsable, certificant la correcta execució dels mateixos així com el compliment dels requeriments i objectius marcats pel client i que hauran de cobrir tot un seguit de necessitats.

- **Arquitecte**: Encarregat de planificar, supervisar i coordinar les activitats d'arquitectura. Referent tecnològic de les activitats d'arquitectura i solucions tecnològiques en l'àmbit dels serveis objecte d'aquesta licitació.

  El personal amb les funcions d'arquitecte haurà de tenir com a principals tasques / responsabilitats:

  - Validar el disseny (a nivell tecnològic) que permeti cobrir totes i cadascuna de les necessitats que vagin apareixent.
  - Aportar, proposar i desenvolupar les millores a nivell d'arquitectura.
  - Conjuntament amb el responsable tècnic, encarregat de donar cobertura a la necessitat de funcions avançades, com a Serveis professionals de tercer nivell en el Suport a disseny de solucions tecnològiques i altres que consideri el CTTI.

- **Administradors**: Responsables de totes les tasques d'administració, procediments i revisió (optimització) de la xarxa (equipament físic, virtual o al cloud), incloent totes les tasques necessàries per l'execució dels serveis definits per a un administrador de xarxa i seguretat.

- **Operadors**: Responsables de totes les tasques d'Operació Bàsica, monitoratge i administració procedimentada de la xarxa.

- **Serveis professionals de tercer nivell:** Encarregat de donar cobertura a totes les fases per a la implantació de la solució. Aquests recursos

estaran a disposició del CTTI per a poder esser utilitzats principalment en les següents casuístiques:

- Suport a disseny de solucions tecnològiques.
- Certificació del disseny proposat.
- Auditoria del desplegament de la solució.
- Agilitzar la interlocutor interna del Fabricant.
- Participació en el procés de preparació i migració de les dades a la nova solució.
- Participació en les tasques d'implantació i posada en servei de la solució, incloent la seva participació en els canvis que es consideri necessari.
- Resolució de les incidències.

3.1.2. Idoneïtat dels perfils

A continuació es detallen els perfils principals amb les característiques mínimes que hauran de tenir, tot i que també haurà d'incloure les funcions descrites a l'apartat 4.1.1 Funcions dels perfils segons correspongui tal i com està detallat a la "4.1.3 Proposta Tècnica i Organitzativa":

- **Responsable de compte**: Haurà de disposar d'una titulació superior que habiliti a realitzar les funcions o experiència mínima de 5 anys en serveis similars del sector públic, en la coordinació i gestió de serveis i projectes i en la relació amb el client, sent la comunicació, la flexibilitat i la proactivitat aptituds fonamentals per aquest perfil.

- **Cap de projecte**: Encarregat de planificar, supervisar i coordinar les activitats dels projectes o servei, realitzar anàlisi de desviacions d'abast, cost i temps, gestionar i fer seguiment dels recursos, dels canvis, riscos i coordinar-se amb altres proveïdors. Realitzarà funcions de direcció, planificació, control i supervisió dels projectes i dels recursos humans assignats a aquests.

  Titulació mínima: Grau o llicenciatura d'àmbit tecnològic que els habiliti a realitzar les funcions requerides.

  Almenys 5 anys d'experiència en tasques de direcció de projectes de xarxes de telecomunicacions.

- **Arquitecte**: Aquest perfil correspon a una persona amb un mínim de 5 anys d'experiència en el disseny d'arquitectures de xarxa similars a la descrita en aquest plec amb experiència en dissenys de xarxes i solucions DDI. Coneixements mínims:

  - Dissenys de xarxes amb els fabricants del servei.
  - Disseny de solucions de arquitectura DDI.

    Aquests coneixements han d'estar acreditats amb alguna certificació vinculada a serveis DDI (DNS/DHCP/IPAM).

- **Administradors**: Aquest perfil correspon a tècnics en administració de xarxes i sistemes amb un mínim de 3 anys d'experiència en xarxes de comunicacions similars a l'especificada en aquest plec amb coneixements en xarxes, solucions DDI, etc. Coneixements mínims:
  - Configuració i Gestió de arquitectures DDI:
    - Administració de usuaris i polítiques d'accés.
    - Configuració en alta disponibilitat del sistema DDI
    - Web APIs (REST/Web Services)
    - Anycast Routing
    - Arquitectures de Sistema DDI:
      - Protocol DHCP i com s'implementa la seva configuració en el Sistema DDI.
      - Protocol DNS i com s'implementa la seva configuració en el Sistema DDI.
      - Protocol NTP i com s'implementa la seva configuració en el Sistema DDI.
      - Eina IPAM i com s'implementa la seva configuració en el Sistema DDI.

    Han de tenir coneixement per executar, entre altres, les següents accions: instal·lació d'equips, upgrade de versió, configuració de clústers, resolució de problemes de connexió, resolució de problemes i incidències, implantació de funcionalitats de seguretat, etc.

    Aquests coneixements han d'estar acreditats amb alguna certificació vinculada a serveis DDI (DNS/DHCP/IPAM).

  - Configuració de xarxes de Routing i Switching:
    - Protocols de routing (IS-IS, OSPF, RIP, EIGRP, BGP) per IPv4 i IPv6.
    - Serveis de nivell 2: Ethernet Virtual Circuits (EVC, QinQ and 802.1ad, EFP), classificació flexible de VLANs, IEEE Bridging, IEEE 802.1s MST, 802.1w RSTP, MST Access Gateway.

    Aquests coneixements han d'estar acreditats amb la certificació mínima o equivalent de Routing & Switching (CCNP).

- **Operadors:** Aquest perfil correspon a tècnics en administració, operació i monitoratge de xarxes i seguretat.
  - Amb un mínim de 2 anys d'experiència en xarxes de comunicacions similars a l'especificada en aquest plec.
  - Titulació mínima: Formació professional de grau mig o grau superior en informàtica o equivalent.

- **Serveis professionals de tercer nivell:** Aquest perfil correspon a un tècnic del fabricant escollit amb les màximes certificacions i experiència per a portar a terme les funcions descrites en aquest plec.

Els licitadors hauran de definir clarament en la seva proposta els recursos que conformaran l'equip, incloent els certificats de fabricant o equivalents i experiència (projectes rellevants) que tinguin tots i cadascun d'ells, , en serveis similars de solucions DDI.

3.1.3. Estructura Organitzativa

A títol orientatiu es presenta el següent equip mínim d'acord:

Classificació perfils	Funcions Perfil	Recurrent
Responsable de Compte	Responsable de Compte	1
Cap de projecte	Cap de projecte	1
Arquitecte	Arquitecte	1
Administrador	Administrador	4
	Serveis professionals de tercer nivel	1
Operador	Operador	2

L'adjudicatari haurà de proporcionar serveis professionals de tercer amb un mínim de 100 hores durant el contracte.

Donada la ràpida evolució de la tecnologia aquest perfils es poden canviar per perfils equivalents necessaris, sempre prèvia validació del CTTI.

Qualsevol canvi en aquests recursos assignats al servei haurà de ser comunicat prèviament al CTTI, que haurà de donar el seu vist i plau, sense el qual no es podrà portar a terme el canvi i per tant l'adjudicatari haurà de buscar una alternativa.

En cas de substitució d'algun altre component de l'equip presentat, el substitut haurà de tenir una idoneïtat equivalent o superior a la presentada en l'oferta.

3.2. Formació

L'adjudicatari haurà de proporcionar els mitjans necessaris per a la formació dels professionals del CTTI i/o professionals de l'àmbit relacionat amb l'objecte contractual, aquesta formació haurà de tenir un mínim de 2 sessions de 8 hores cadascuna o equivalent.

Aquesta formació cobrirà els següents aspectes:

- Formació en els equips, serveis, funcionalitats, operació i eines implantades, aplicables al disseny escollit. Altres funcionalitats dels equips i serveis.
- Aspectes rellevants dels procediments del fabricant; roadmap, consultes tècniques, cicle de vida dels productes, contractes de manteniments, etc
- Manuals d'usuari del servei amb informació detallada de les prestacions i funcionalitats.

- Documentació de processos, base de dades de coneixement, etc.
- Disponibilitat contínua via web.

Tota la formació i documentació necessària serà proporcionada, almenys, en català.

4. Acords de nivell de servei (ANS)

4.1. Objectiu

Es descriu el model d'Acord de Nivell de Servei (en endavant ANS), que defineix els indicadors i els nivells de servei exigits, i estableix una base objectiva i mesurable que reflecteixi el compromís entre l'adjudicatari i el CTTI per prestar els serveis requerits de forma satisfactòria a la Generalitat de Catalunya.

El CTTI pretén obtenir un nivell de servei d'alta qualitat, així com un grau de satisfacció elevat per part dels usuaris, basat en:

• L'establiment d'indicadors de servei, de manera que el CTTI pugui realitzar una avaluació objectiva del servei i els seus lliurables, i que l'adjudicatari tingui una base per a la correcció de les eventuals deficiències en la prestació, i per a la millora dels seus processos i organització.

• L'establiment d'un model de penalitzacions que relacioni el nivell de prestació del servei amb la seva facturació.

• L'establiment d'indicadors que permetin mesurar el grau de satisfacció percebuda pels usuaris del servei.

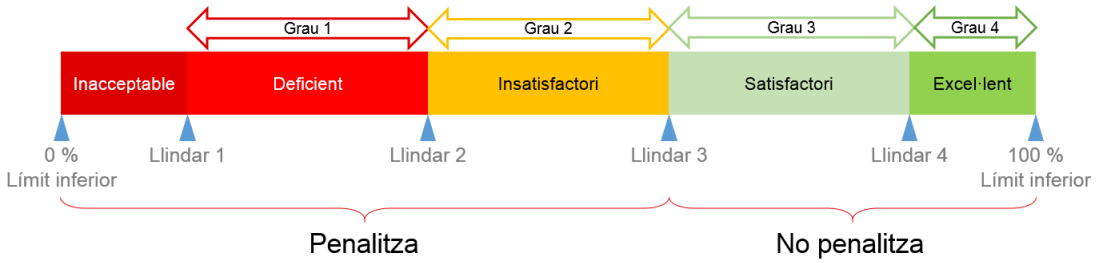
A l'Annex 1. ANS del present plec es troben els indicadors de servei definits pels serveis descrits en aquest document. Els indicadors que hi consten s'aplicaran en el càlcul de les penalitzacions per incompliment del llindar mínim requerit com s'explica a continuació.

4.2. Característiques dels indicadors

Els indicadors tindran les següents característiques:

- **Codi**. Identificador únic de l'indicador.
- **Nom**. Defineix l'objecte de mesura de l'indicador.
- **Descripció**. Descripció de l'indicador i el seu objectiu. S'inclouen les restriccions necessàries per dur a terme el càlcul del valor de l'indicador (per exemple, restriccions horàries, tipificació dels incidents, etc.).
- **Categoria**. Agrupa diferents ANS d'un mateix tipus. Per exemple: Consultes, Gestió de Peticions, Gestió d'incidències, Gestió d'Inventari.
- **Fórmula d'obtenció/eina**. Fórmula a aplicar pel càlcul del valor de l'indicador de mesura, identificant les variables que intervenen al càlcul (mètriques) i, si escau, la referència a l'eina que permet l'automatització i extracció de les dades.
- **Periodicitat**. Freqüència de mesura del valor de l'indicador.

- **Llindars de grau per a la definició dels trams**. Valors que defineixen el grau de compliment del nivell de servei exigit. Per a cada indicador es definiran 4 llindars de grau. En funció de la banda en què es trobi l'indicador presentarà els valors següents:



- **Penalització màxima (PPMax).** Determina el valor màxim al qual pot arribar la penalització en el cas d'incompliment del llindar objectiu definit.

4.2.1. Grau de l'indicador

El grau de l'indicador pot prendre els següents valors:

Grau	Valor
1	Deficient o Inacceptable
2	Insatisfactori
3	Satisfactori
4	Excel·lent

El grau 4 serà el nivell objectiu, mentre que el grau 3 serà el nivell d'acompliment mínim per considerar que l'indicador és satisfactori.

4.3. Càlcul dels indicadors

Per tot indicador s'estableixen 4 llindars per definir els trams lineals que han de permetre l'obtenció del grau associat.

	Llindar Grau 1	Llindar Grau 2	Llindar Grau 3	Llindar Grau 4
Indicador de mesura	Valor 1	Valor 2	Valor 3	Valor 4

- Pel valor mesurat per un indicador (valor indicador), s'haurà de cercar entre quins llindars es troba i aplicar el següent procediment, tenint en compte si els valors definits pels llindars (Valor 1 – Valor 4) són creixents o decreixents:
- Per valors de llindars creixents (valor Llindar Grau 1 < valor Llindar Grau 4).
- Si el valor és inferior al llindar 1, el grau serà 1.
- Si el valor és igual o superior al llindar 4, el grau serà 4.
- En la resta de casos s'aplicarà la fórmula de càlcul del grau.
- Per valors de llindars decreixents (valor Llindar Grau 1 > valor Llindar Grau 4).
- Si el valor és superior al llindar 1, el grau serà 1.
- Si el valor és igual o inferior al llindar 4, el grau serà 4.
- En la resta de casos s'aplicarà la fórmula de càlcul del grau.

4.3.1. Fórmula de càlcul del grau

$$Grau = \frac{(Valor\ indicador - Valor\ llindar\ inferior)}{(\text{Valor llindar superior} - \text{Valor llindar inferior})} + Grau\ corresponent\ al\ llindar\ inferior$$

En aplicar la fórmula de càlcul del grau, cal tenir en compte les següents consideracions:

- Quan dos o més llindars prenen el mateix valor, el valor del "Grau corresponent al llindar inferior" correspon al del llindar coincident superior.

Per exemple, quan el Llindar Grau 1 i el Llindar Grau 2 prenen el mateix valor, el "Grau corresponent al llindar inferior" correspon al del Llindar Grau 2, és a dir, pren valor 2.

- Quan el valor mesurat per un indicador (valor indicador) coincideix amb algun dels valors definits pels llindars (Valor 1, Valor 2, Valor 3), es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident. Quan dos o més llindars prenen el mateix valor, es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident superior.

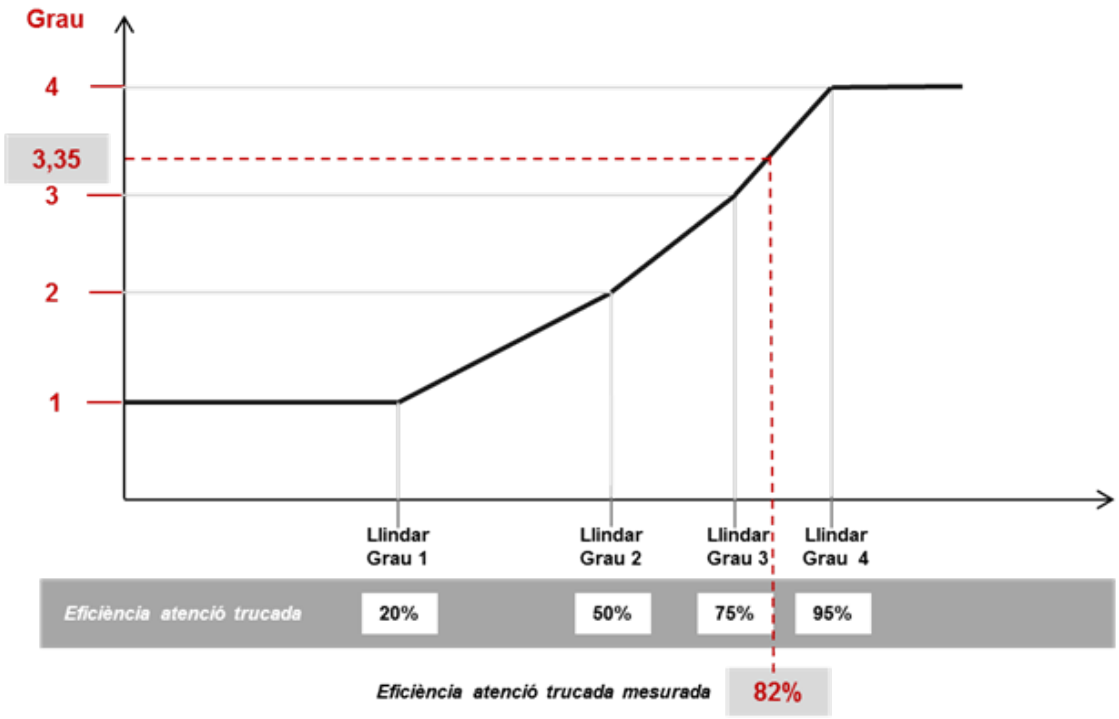
Per exemple, suposant els següents valors de llindars: Llindar Grau 1 i el Llindar Grau 2 prenen el mateix valor, 20%, Llindar Grau 3 pren valor 75% i Llindar Grau 4 pren valor 95%; quan el valor mesurat per l'indicador pren valor 20%, el "Valor llindar inferior" pren valor 20%, el "Valor llindar superior" pren valor 75% i el "Grau corresponent al llindar inferior" pren valor 2.

4.3.2. Exemple de càlcul

Suposem que tenim l'indicador "Eficiència atenció trucada" que pot prendre valors percentuals entre 0% i 100% i que el valor objectiu és 95%. Si s'han definit els següents llindars:

Llindar Grau	Valor de l'indicador
1	20%
2	50%
3	75%
4	95%

Si el valor mesurat en un període per l'indicador "Eficiència atenció trucada" ha estat 82%, el grau calculat és: ((82-75)/(95-75))+3=3,35.



Aquest model és dinàmic, ja que permet adaptar-se en el temps a nous nivells objectius i nivells mínims, sense variar els graus possibles.

4.4. Relació d'ANS

A l'*Annex 1. ANS* es troben els indicadors definits pels serveis descrits en aquest document. Els indicadors que hi consten s'aplicaran en el càlcul de les penalitzacions per incompliment del llindar mínim requerit com s'ha explicat anteriorment.

4.5. Fonts d'informació per a l'obtenció dels nivells de servei

El CTTI emprarà el sistema d'informació CONTIC (Control d'acord de nivell de servei TIC) per al càlcul, anàlisi i emmagatzemament d'indicadors de servei i de procés. Tot i que a l'inici del servei el sistema d'informació CONTIC no sigui capaç de calcular tots els indicadors definits, s'aniran incorporant progressivament al seu catàleg. El proveïdor haurà de proveir els indicadors que estiguin sota la seva responsabilitat a través de les interfícies habilitades.

Sempre que sigui possible, l'origen de les dades utilitzat per al càlcul dels indicadors seran les eines de gestió dels tiquets i monitoratge del CTTI. Per aquells indicadors que el CTTI no sigui capaç d'obtenir de manera autònoma, serà responsabilitat de l'adjudicatari calcular-los i reportar-los amb la periodicitat establerta i el detall i format que requereixi el CTTI, podent arribar a nivell d'instància de servei o de tiquet.

El CTTI utilitzarà els indicadors de servei per realitzar els càlculs de compliment dels ANS i per generar els informes corresponents.

4.6. Modificació dels indicadors i nivells de servei

Al llarg de la prestació del contracte, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei, el CTTI conjuntament amb el proveïdor consensuaran i planificaran la seva modificació.

Algunes de les causes que poden comportar aquestes modificacions són, entre d'altres, les variacions d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, les innovacions i les millores del servei.

4.7. Aplicació dels acords de nivell de servei

Els Acords de Nivell de Servei seran d'obligat compliment al llarg del contracte, excepte que per causes de força major o circumstàncies excepcionals, i sempre d'acord entre l'adjudicatari i el CTTI, es podrà decidir la no obligatorietat del compliment dels Acords de Nivell de Servei, en alguns o en tots els indicadors.

4.8. Pla de millora en cas d'incompliment reiterat dels ANS

En cas d'incompliment reiterat dels Acords de Nivell de Servei, durant un període de 3 mesos consecutius o 3 mesos alternats en un període de 6 mesos, el proveïdor estarà obligat a presentar un pla de millora del servei amb l'objectiu d'assolir el compliment dels ANS. S'entén com a incompliment dels ANS que un 25% o més dels indicadors de mesura relacionats a l'Annex 1. ANS estiguin per sota del llindar 3.

El pla de millora s'haurà de presentar en un termini de 2 setmanes a partir que es compleixi la condició anterior i, un cop validat pel CTTI, s'executarà amb els mitjans propis de l'adjudicatari, sense que aquesta pugui repercutir-ne el cost al CTTI ni dedicar els recursos del servei de forma significativa.

El pla de millora haurà de permetre el compliment dels ANS en un termini màxim de 2 mesos.

La falta de presentació del pla de millora en el termini fixat, o el no compliment dels ANS en el termini màxim indicat, serà causa de resolució del contracte.

5. Model de relació

Per defecte, el model de relació i l'estructura de comitès que s'implementarà per la governança específica del serveis objecte d'aquest contracte basat són els detallats en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20164 que regeix l'acord marc pels subministraments i projectes de xarxa de la Generalitat de Catalunya.