# Informe tècnic de valoració de les ofertes presentades al procediment de contractació relativa a “Servei de ciberseguretat gestionada per a la Universitat Oberta de Catalunya”

## Expedient HSE000013/2019

En data 25 de juny de 2019, el Director General de la Universitat Oberta de Catalunya, el Sr. Antoni Cahner Monzó, en la seva condició d'Òrgan de Contractació, va acordar iniciar el procediment de contractació relatiu al “Servei de ciberseguretat gestionada per a la Universitat Oberta de Catalunya”.

La convocatòria d'aquest procediment es va publicar en data 5 de setembre de 2019 al Perfil del Contractant d'aquesta entitat. Igualment, la convocatòria d'aquest procediment va enviar-se al Diari Oficial de la Unió Europea el dia 2 de setembre de 2019. Així mateix, el termini fixat per a la presentació de les proposicions era el 7 d´octubre de 2019 a les 17 hores.

Van presentar oferta en el termini establert les següents empreses:

- ERNST & YOUNG Global Limited
- Viewnext
- IThink UPC
- (UTE) Opentrends + Cybernforce + Proficio
- PricewaterhouseCoopers PwC
- S2Grupo
- S21Sec
- SAYTEL SERVICIOS INFORMÁTICOS SA
- T-Systems

En data 9 d´octubre de 2019 es va procedir en acte no públic de la Mesa de Contractació de la UOC a l'obertura i revisió de la documentació continguda en el Sobre núm. 1 relativa a la documentació general.

Segons consta en l'acta de constitució de la Mesa de Contractació i de qualificació de la documentació general, les empreses Saytel Servicios Informáticos SA i Ernst&Young, SL van presentar la documentació de forma correcta i van ser admeses al procediment. Per altra banda, les empreses Grupo 21SEC Gestión SA, IthinkUPC SLU, S2 Grupo de Innovación en

Procesos Organizativos SLU, T-Systems ITC SAU, UTE Opentrends - Cybernforce - Proficio, Viewnext SA, UTE Pricewaterhousecoopers Auditores SL & Pricewaterhousecoopers Asesores de Negocios SL van presentar les ofertes amb defectes esmenables. Totes elles van presentar els aclaramients de forma correcta i, per tant, va ser admesa al procediment.

En data 25 d´octubre de 2019 es va procedir a l'obertura pública del sobre núm. 2 que conté les propostes tècniques formulades per les empreses, la valoració de les quals depèn d'un judici de valor.

A continuació, es procedeix per mitjà del present document a valorar l'oferta tècnica del sobre núm. 2 de les empreses admeses a licitació.

# Proposta tècnica

De conformitat amb l'establert al Plec de Clàusules Particulars, els criteris d'adjudicació que s'han d'aplicar per valorar les ofertes presentades a la contractació que aquí ens ocupa són aquells recollits a l'apartat M del Quadre de referències, els quals es detallen a continuació:

| **Taula de puntuació** | |
|---|---|
| **Puntuació màxima** | **40 punts** |
| 1. Proposta de prestació del servei | **30 punts** |
| 1.1. Detecció, anàlisi i gestió de vulnerabilitats | **6 punts** |
| A. Solució proposada | 3 punts |
| B. Recursos assignats | 3 punts |
| 1.2. Gestió i resposta a incidents de seguretat de la informació CSIRT | **6 punts** |
| A. Solució proposada | 3 punts |
| B.. Recursos assignats | 3 punts |
| 1.3. Anàlisi de malware | **6 punts** |
| A. Solució proposada | 3 punts |
| B. Recursos assignats | 3 punts |
| 1.4. Anàlisi forense | **6 punts** |
| A. Solució proposada | 3 punts |
| B. Recursos assignats | 3 punts |
| 1.5. Manteniment, revisió, administració i reporting de la infraestructura de seguretat de la UOC | **6 punts** |
| A. Solució proposada | 3 punts |
| B. Recursos assignats | 3 punts |
| 2. Gestió i governança del servei | **5 punts** |
| 2.1. Model de relació | 1punt |
| 2.2. Metodologia, mecanismes de control i seguiment del servei | 3 punts |
| 2.3. Eines | 1 punt |
| 3. Fases de la prestació del servei | **5 punts** |
| 3.1. Auditoria i Transformació | 2 punts |
| 3.2. Servei regular | 1 punt |
| 3.3. Devolució del servei | 2 punts |

Per poder valorar cadascun dels conceptes de la valoració subjectiva es tindran en compte els següents criteris:

**1. Proposta de prestació del servei (fins a un màxim de 30 punts):**

Cadascuna de les cinc tasques tipificades puntuarà un màxim de 6 punts:

● Detecció, anàlisi i gestió de vulnerabilitats (6 punts)
● Gestió i resposta a incidents de seguretat de la informació CSIRT (6 punts)
● Anàlisi de malware (6 punts)
● Anàlisi forense (6 punts)
● Manteniment, revisió, administració i reporting de la infraestructura de seguretat de la UOC (6 punts)

Per a cadascun dels 5 apartats sol·licitats es valorarà:

● **Solució proposada (fins a un màxim de 3 punts)**

Es valorarà la coherència i el detall de la proposta tècnica i organitzativa per a la prestació del servei de seguretat, així com la identificació de forma ràpida del compliment individual dels requeriments funcionals i tecnològics indicats en el plec de prescripcions tècniques, valorant la comprensió del problema, la capacitat i la qualitat de la informació presentada.
No es valorarà la simple transcripció del plec tècnic

Criteris puntuació Solució Proposada:

- 3 punts: La proposta inclou:
  - Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades que permeti assolir els requeriments funcionals i tecnològics indicats en el plec
  - I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

- 1 punt: La proposta inclou:
  - Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.
  - I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme

per l'àmbit valorat.

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

**● Recursos assignats. (fins a un màxim de 3 punts)**

Es valorarà la identificació clara dels recursos assignats, dedicació i funcions de cada un dels perfils proposats d'acord a les tasques a executar. La idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.
No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Recursos assignats:

● 3 punts: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:
- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

● 1 punts: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:
- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
  Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

**2. Gestió i governança del servei (fins a un màxim de 5 punts):**

Concretament es valorarà:

**● Model de relació (fins a un màxim de 1 punt).**

Es valorarà el grau de detall en la descripció del model de relació i l'estructura dels comitès proposats, incloent les funcions, periodicitat de les reunions, entregables i el seu contingut.
No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Model de relació:

- 1 punt: Si la proposta inclou:
    - Les funcions de cadascun d´ells
    - Les figures implicades
    - La seva periodicitat
    - Entregables a lliurar per part del proveïdor adjudicatari així com el seu contingut.

- 0,5 punts: Si la proposta inclou:
    - Una descripció detallada del model de relació, on s´inclou:
    - La figura de coordinació del servei i les seves funcions
    - Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.
    - I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

- 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

- **Metodologia, mecanismes de control i seguiment del servei (fins a un màxim de 3 punts)**

Es valorarà la metodologia i els mecanismes de control i seguiment en relació a la naturalesa del servei i als requeriments del plec. Metodologia d'identificació i gestió de riscos.
No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Metodologia, mecanismes de control i seguiment del servei:

- 3 punts: La proposta inclou:
    - Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.
    - I, una descripció detallada dels mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció i gestió de riscos, etc.)

- 1 punt: La proposta inclou:
    - Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.
    - La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials

per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

**● Eines. (fins un màxim de 1 punt)**

Es valorarà el conjunt d'eines aportades pels licitadors, addicionals a les disponibles per part de la UOC, enfocades a facilitar i millorar la prestació del servei. Per cadascuna de les eines proposades es valorarà:

- Idoneïtat de les eines aportades pels licitants, valorant les capacitats aportades i l'adaptació a les necessitats reals de la UOC.
- Descripció de les funcionalitats de les eines proposades. Es valorarà el detall en la descripció de les funcionalitats, la facilitat d'ús i els serveis que s'hi puguin monitoritzar en temps real.
- Detall de la planificació prevista per la posta en funcionament de les eines.
- No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Eines:

● 1 punt: La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.
- I, la idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau de servei.
- I el detall de la planificació prevista per la posada en funcionament de les eines.

● 0,5 punts: La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.
- La proposta no inclou:
  - La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
  - O, el detall de la planificació prevista de la posada en funcionament de les eines.

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

**3. Fases de la prestació del servei (fins a un màxim de 5 punts)**

Concretament es valorarà:

**● Auditoria i Transformació (fins a un màxim de 2 punts)**

Es valorarà el detall de la proposta tècnica i organitzativa de la definició dels processos de les fases d'auditoria i de transformació del servei. Així mateix, es valorarà també la metodologia utilitzada i el nombre de recursos dedicats i dels seus perfils.
No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Auditoria i transformació:

- 2 punts: La proposta inclou:
  Una descripció detallada de la proposta tècnica, on s´inclou:
  La definició dels processos i fites que permetin assolir la fase d´auditoria i transformació.
  Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
  I, una descripció detallada de la proposta organitzativa, on s´inclou:
    La metodologia utilitzada
    El nombre de recursos que es dedicaran així com els seus perfils.
- 1 punt: La proposta inclou:
  Una descripció detallada de la proposta tècnica, on s´inclou:
  La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
  Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
  I, una descripció detallada de la proposta organitzativa, on s´inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

- 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

- **Servei regular (fins un màxim de 1 punt).**

Es valorarà una proposta de millora contínua que aporti els mecanismes adequats per garantir l'estabilitat del servei, la detecció temprana de riscos i els mecanismes per evidenciar els resultats de l´aplicació del pla de millora.
No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Servei regular:

- 1 punt: La proposta inclou una proposta de millora contínua completa detallant:
  - Els mecanismes necessaris per tal de garantir l'estabilitat del servei
  - Els mecanismes per tal d´identificar una detecció temprana de riscos
  - Mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

- 0,5 punts: La proposta inclou:
  - Una proposta de millora contínua, on es detallen els mecanismes

necessaris per tal de garantir l'estabilitat del servei
- La proposta no inclou:
  - Els mecanismes per tal d'identificar una detecció temprana de riscos
  - Ni els mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

**● Devolució del servei.(fins un màxim de 2 punts)**

Es valorarà la metodologia i documentació proposada per a la transferència del coneixement (per assegurar la continuïtat del servei) i els terminis establerts, en funció del grau de detall i idoneïtat:

- Metodologia del pla de devolució.
- Mitjans compromesos per la devolució (qualitat i idoneïtat de l'equip proposat).
- Durada compromesa de l'equip.
- La informació lliurada cobreix tots els àmbits i processos del servei.
- No es valorarà la simple transcripció del plec tècnic

Criteris de puntuació Devolució del servei:

● 2 punts: La proposta inclou:
- Una descripció detallada de la metodologia corresponent a la fase de devolució.
- I, els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
- I, la durada compromesa de l´equip.
- I, entrega d´informes que cobreixin tots els àmbits i processos del servei.

● 1 punt:
- La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
- La proposta no inclou:
  - Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
  - Ni la durada compromesa de l´equip de treball.
  - Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

● 0 punts: Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

# 1. Proposta de prestació del servei (fins a 30 punts)

## 1.1. Detecció, anàlisi i gestió de vulnerabilitats (fins a 6 punts)

### 1.1.1 ERNST & YOUNG Global Limited

#### A: Solució proposada (fins a 3 punts)

La proposta inclou una descripció detallada dels procediments associats al servei: Descobriment, Avaluació del nivell de la criticitat, Gestió de la resolució i Registre i seguiment. Tots ells són correctes i s'ajusten perfectament al cicle de vida de la gestió de les vulnerabilitats.

El licitador proposa l'ús d'un conjunt ampli d'eines, tant de software lliure com en format propietari. Aquestes eines proposades són: Nessus, JIRA (UOC), One Trust, Webinspect, Kiwan, Defect Dojo, Burpsuite Pro, Kali / Nmap, Altres eines propietàries d'EY.

Les metodologies proposades s'ajusten perfectament a les requerides en el plec, tant pel que fa a l'anàlisi de vulnerabilitats com la gestió i la valoració de les mateixes. EY ha desenvolupat una metodologia d'anàlisi de seguretat pròpia basada en dues metodologies internacionalment reconegudes, com són OSSTMM (Open Source Security Methodology Manual) i OWASP (Opensource Web Application Security Project), juntament al sistema de mesurament de criticitat de vulnerabilitats CVSSv2 (Common Vulnerability).

Les fases queden cobertes perfectament amb l'explicació proposada pel licitador, cobrint les necessitats demanades en el plec. Aquestes fases proposades pel licitador són: Anàlisi i validació de resultats dels escanejos, Generació de registres de resultats, Consultes d'historials d'anàlisi de cada actiu, Revisió continuada de les publicacions de vulnerabilitats descobertes, Consulta d'inventaris d'actius. (CMDB, SSCM, Exchange, MDM), Anàlisi periòdic d'actius per trobar aquells que necessiten l'aplicació de pegats correctius, Anàlisi de vulnerabilitats sota demanda per tal de saber si un actiu necessita l'aplicació d'una actualització o pegat. Pel que fa a les fites aquestes queden especificades dins el calendari proposat pel licitador i són: Connexió EY Cybersecurity Operations Center, Accessos a eines de la UOC i Requeriments per l'escaneig de vulnerabilitats, Parametrització d'eines d'escaneig i gestió de vulnerabilitats d'EY, Reconeixement de context i inventaris, Definició del pla anual d'escanejos i activitat per identificació de vulnerabilitats, Escaneig / auditoria completa per la identificació de vulnerabilitats, Escaneig / auditoria sota demanda o específica de recheck, Reporting, priorització i comunicació de les vulnerabilitats identificades i plans d'acció, Suport i seguiment de la resolució amb equips resolutors, Reporting de l'estat de resolució de les vulnerabilitats identificades i Pla d'evolució trimestral i seguiment de les accions d'evolució executades.

Per últim, la proposta inclou també un calendari al final de l'apartat “Proposta de prestació del Servei”, que compleix els requeriments de la UOC.

El licitador fa una descripció canònica i formal del servei demanat. La proposta és ordenada, metòdica en l'explicació, coherent i s'ajusta a tots els requeriments del plec i cobreix completament amb les

necessitats demanades en el PPT.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

La proposta inclou una descripció detallada dels recursos assignats. Hi ha un perfil específic de "Especialista" en resposta a incidents de seguretat de la informació. Aquests perfils es composen de:

- COORDINADOR DEL SERVEI DE SEGURETAT amb les funcions de: Realitzar el seguiment del servei continuat i de les activitats que poden ser peticionades de manera discreta. Seguir i gestionar possibles desviacions de la planificació i pressupost. Coordinar el compliment de calendaris, fites, superació de barreres i implicació dels actors involucrats. Consolidar i aportar iniciatives que permetin la presa de decisions operatives i estratègiques. Realitzar el reporting del servei. Donar suport a la realització / verificació d'estimacions de nous serveis dins del manteniment evolutiu. Gestionar adequadament la demanda del servei per tal d'assegurar l'adaptabilitat i la màxima qualitat.

- TÈCNIC ESPECIALISTA EN HACKING ÈTIC I PENTESTING per a: Planificar, preparar i programar les actuacions per la identificació de vulnerabilitats. Anàlisi i eliminació de falsos positius dels resultats obtinguts. Cerca proactiva de vulnerabilitats a la infraestructura de la UOC. Consulta de l'historial d'anàlisi de cada actiu. Anàlisi periòdic dels actius per trobar aquells que requereixen l'aplicació de pegats correctors. Anàlisi d'afectació de les vulnerabilitats en els actius de la infraestructura. Sol·licitud d'aplicació de contramesures. Comprovació de la correcta aplicació de les accions correctores.

- AUDITOR DE SEGURETAT DE LA INFORMACIÓ amb les següents funcions: Suport a l'auditoria inicial a realitzar com a primera fase del servei de seguretat gestionada. Executar i coordinar els projectes d'auditoria tant de marc normatiu com de compliment legal (evolució i millora). Documentar i presentar els resultats de les auditories d'acord amb el sistema i metodologia de valoració i de reportat establert. Incorporar i mantenir la informació de les auditories a OneTrust..

- PROFESSIONAL CERTIFICAT EN SEGURETAT DE LA INFORMACIÓ per al: Suport en la definició, transformació, industrialització i formalització organitzativa de les diferents tasques del servei de seguretat gestionada. Suport en la definició, evolució, desplegament i seguiment d'un model de gestió de la seguretat de la informació per la UOC. Identificació d'oportunitats de millora i riscos en la gestió de seguretat en base a millors pràctiques. Execució de projectes de seguretat de la informació en l'àmbit de la consultoria. Suport a tasques de realització de quadres de comandament.

La dedicació i les hores estan ben detallades fent un total de 380 hores anuals. Juntament amb la dedicació del coordinador del servei i de l'auditor (236 hores/any) fa que el dimensionament sigui correcte i suficient.

La proposta presenta una identificació dels recursos molt ben detallada. Els perfils estan clarament identificats, així com les funcions que realitzarà. Es millora considerablement el número d'hores proposades per perfil.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

### 1.1.2 Viewnext

#### A: Solució proposada (fins a 3 punts)

El licitador fa una descripció correcta, basant-se en l'execució, per poder prestar el servei, de quatre mòduls: Inspecció de xarxa, Identificació dels serveis dels sistemes, Anàlisi de la infraestructura de comunicacions i en la Cerca i verificació de vulnerabilitats.

Els procediments associats a les fases són correctes i estan citats. Aquests procediments que cita el licitador són: Conèixer els principals riscos tecnològics als que s'enfronta la UOC, Identificar els punts d'entrada a la organització, Disposar dels resultats per objectivitzar i prioritzar les decisions i inversions en sistemes, Disposar d'un pla d'accions correctives que protegeixin els actius del negoci, Disminuir a curt. mig i llarg termini el risc degut a incidents de seguretat de la informació.

Per a cadascun d'aquests procediments el licitador no en fa cap descripció.

El licitador proposa i cita l'ús d'eines únicament en la fase de "Cerca i verificació de vulnerabilitats". Les eines citades en la oferta són: AppScan, Nessus Professional, OpenVAS i en tot cas aquelles que tinguin la qualificació de "Approved Scanning Vendor (AVS)", sense donar més informació al respecte d'una forma més concreta.

S'expliquen les metodologies que es faran servir, i es descriuen els mòduls que s'executaran en la metodologia escollida. Aquestes s'ajusten perfectament a les que hi ha requerides en el plec. Les metodologies citades són: Open Source Security Testing Methodology Manual (OSSTMM) i la Information System Security Assessment Framework (ISSAF).

No s'ha trobat cap calendari proposat per aquest servei dins la oferta.

Les fases estan explicades correctament, encara que en alguns casos com el "Compliment de les polítiques de seguretat", "l'Anàlisi inicial i la presa de dades" o la "Mitigació" es troba a faltar una descripció del nivell d'implicació, dels mitjans tècnics i humans i les hores de dedicació. Les fases que proposa el licitador són: Anàlisi inicial i presa de dades, Auditoria de ciberseguretat, Informe final i Mitigació

No s'han localitzat descrites les fites associades al servei.

La proposta està correctament explicada, encara que amb algunes mancances de detall, tal i com s´ha explicat anteriorment., com per exemple la inexistència de calendari i la descripció de les fites. Es descriu un ventall escàs d'eines a utilitzar focalitzat només en els procediments de Cerca i Verificació de vulnerabilitats .

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

La proposta inclou els perfils assignats al servei. Les funcions, encara que descrites, haurien de ser més detallades per tots els perfils, però en especial per al de "AUDITOR", ja que es consideren molt genèriques. Aquestes funcions assignades són:

> -COORDINADOR DE SERVICIO: Es responsabilitza de la gestió i seguiment de totes les tasques desenvolupades en el SOC del licitador.
>
> -AUDITOR EXPERTO: Responsable del seguiment operatiu del servei, Responsable de la supervisió i coordinació del servei, Realització dels informes, Preparació i assistència a les reunions de seguiment, Presentació d'informes, Anàlisi de millores i recomanacions, garantir que les eines usades estan del tot actualitzades i operatives i la Gestió del cicle de vida de les vulnerabilitats.
>
> -AUDITOR Elaboració i manteniment de tota la documentació tècnica elaborada.

La dedicació i les hores no estan ben detallades i es marca que s'estableix en el 100% de les hores de l'auditor en horari laboral i un 20% de les hores de l'expert que podran executar-se fora de l'horari laboral en cas de necessitat, però no s'estableix sobre què s'aplica el percentatge.

El dimensionament és correcte però la proposta no especifica sobre quin total aplica el percentatge de dedicació de les hores ofertades.

La proposta presenta una identificació dels recursos, així com les funcions que realitzaran cadascun d´ells, tot i que els perfils no estan clarament identificats.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.3. IThink UPC

### A: Solució proposada (fins a 3 punts)

Els procediments associats són correctes i s'ajusten perfectament a les activitats proposades en el plec per la UOC. En resum aquests procediments proposats són: Preparació (revisió de l'abast i avís a persones involucrades), Escaneig (automàtic i validació manual), Remediació (priorització de vulnerabilitats i aplicació de solucions ) i Re-escaneig (validació de la correcta solució) i Un pas inicial addicional una vegada durant l'inici del projecte on s'hauran de definir diversos paràmetres i fer el setup de les eines.

El nombre i la qualitat de les eines s'ajusta perfectament a les necessitats de la UOC i la combinació entre eines en codi lliure i eines de pagament fa que siguin perfectament assumibles. Les eines proposades pel licitador són: Nessus Professional, Acunetix, Nmap, Kali Linux, BurpSuite Professional, OWASP ZAP, Nikto, Metasploit, i altres eines per validacions manuals: ncat, sslscan, metasploit, curl, etc.

Les metodologies proposades són correctes i s'ajusten a les activitats a realitzar dins del marc de la prestació d'aquest servei. Aquestes metodologies es cita que seran les propugnades per SANS i NIST.

La proposta té un calendari ben estructurat que planifica una sèrie d'activitats que encaixen en les activitats plantejades en el plec.

Les fases són correctes s'ajusten amb la metodologia proposada i tenen una correspondència directa amb el calendari plantejat i les fites posteriors. Aquestes fases són: la Fase de Preparació, Fase De Detecció de Vulnerabilitats, Fase de Remediació i Fase de Verificació.

Les fites són correctes i es valora positivament que una d'elles plantegi la creació, reporting i revisió per part d'un Comitè Estratègic de la UOC amb la participació del licitador. En resum la llista de fites associades al calendari és: Inici del servei i posar en marxa el protocol, Resultat "satisfactori" a les enquestes sobre les activitats realitzades i l'informe executiu amb les tres anàlisis per any, Revisió satisfactòria en el Comitè Estratègic i reflexió sobre possibles modificacions i Avenços observables en matèria de gestió de vulnerabilitats.

La proposta es considera apropiada ja que dona compliment als requisits valorats en aquest apartat i es valora positivament que es plantegin fites estratègiques.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta inclou els perfils assignats als servei així com les seves funcions, les quals són:

- Un Coordinador del servei amb les funcions de seguiment del servei i de gestió de la demanda. També en funcions d'interlocució i planificació. Així com vetllar per l'aprovisionament correcte del servei més el seguiment.

- Quatre especialistes de seguretat amb funcions de: Anàlisi de vulnerabilitats, Validació de la remediació, Recomanacions específiques, Validació de l'inventari, Execució dels escanejos automàtics i Suport a la documentació.

Les hores de dedicació són correctes i es proposa un plus sobre el plec fent un total de 240 + 36 anuals. Les funcions i el dimensionament estan ben determinades per les fases i procediments descrits abans i són satisfactoris.

La proposta presenta una identificació dels recursos i les seves funcions molt detallada. Els perfils estan clarament identificats, així com les funcions que realitzaran.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.4. (UTE) Opentrends + Cybernforce + Proficio

### A: Solució proposada (fins a 3 punts)

El licitador basa la resposta d'aquest apartat en una eina propietat de la companyia Proficio que ofereix opcionalment l'anàlisi de vulnerabilitats.

No s'han trobat descrits procediments associats al servei.

La proposta indica que l'eina que utilitzarà per executar el servei és el producte anomenat Proficio ProSCAN.

No s'ha pogut evidenciar l'existència de metodologies associades al servei.

No hi ha un calendari proposat per aquest servei.

Tampoc s'ha pogut trobar cap llista o descripció de les fases que hi hauria d'haver associades al servei.

No s'han pogut trobar fites associades al servei.

La proposta és incompleta, no cobrint la majoria dels elements demanats per aquest servei.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta del licitador no s'identifiquen els recursos assignats, ni descriu la dedicació i funcions de cada un dels perfil, per tant, tampoc es pot avaluar el correcte dimensionament dels recursos.

- **0 punts**: La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

## 1.1.5. PricewaterhouseCoopers PwC

### A: Solució proposada (fins a 3 punts)

El licitador fa una descripció correcta del servei amb un contingut extens i detallat. Es parla de fer un anàlisi des de dos possibles perspectives: Caixa negra i/o Caixa blanca.

Els procediments associats són correctes, estan molt ben estructurats i abasten tots els aspectes relacionats amb la gestió de les vulnerabilitats. Tots els procediments cobreixen amb escreix les activitats detallades en el plec a més són coherents amb la metodologia proposada. Aquest procediments de gestió de les vulnerabilitats en resum són: Planificación, Análisis, Mitigación, Verificación, Reporting.

El licitador proposa 3 eines per anàlisi automàtic de vulnerabilitats: Tenable Nessus Scanner, Burp Suite Professional i Acunetix. Es troba a faltar una descripció més àmplia especialment en la fase d'Anàlisi Manual de vulnerabilitats d'Infraestructura i de Serveis Publicats.

Les metodologies proposades s'ajusten perfectament a les requerides en el plec, s'utilitzaran metodologies reconegudes i avalades internacionalment. Bàsicament les que proposen a usar són: OSSTMM i OWASP.

La proposta inclou un calendari i unes fites associades al mateix que compleix els requeriments de la UOC.

Les fases del servei estan correctament definides i de forma extensa, donant resposta al plec. Aquestes fases, en resum, són: Recopilació de la informació que exposa la nostra organització, Identificació dels diferents elements, interfícies i serveis de xarxa existents, Anàlisi i identificació automàtica de les possibles vulnerabilitats, Anàlisi manual de les vulnerabilitats de la infraestructura, Anàlisi dels serveis publicats i el Procés de gestió de les vulnerabilitats.

Les fites són correctes i tenen una correspondència amb el calendari proposat. Aquestes són: Anàlisi del procés actual, Desenvolupament i millora del procés, Definició del pla d'assaigs i revisions, Escanejos de vulnerabilitats, Test d'Intrusió i Gestió de vulnerabilitats.

La proposta està ben detallada i les fases correctament desenvolupades. No obstant, s'ha trobat a faltar un ventall més ampli d'eines.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els recursos estan correctament identificats mitjançant el seu perfil i les funcions i dedicació estan llistades amb suficient detall, donant compliment al que requereix el servei.

Aquests perfils i funcions són:

- Un Coordinador del servei: Definir el pla d'escanejos i revisions així com Coordinar el servei.

- Un perfil Especialista en Hacking Ètic i Pentesting: Per realitzar els Escanejos de vulnerabilitats, els Test d'Intrusió i la Gestió de les vulnerabilitats.

- Un perfil Auditor en Seguretat de la Informació i Continuïtat de Negoci: per l'Anàlisi del procés actual i el Desenvolupament i Millora del Procés.

- Un perfil Certificat en Seguretat de la Informació: per l'Anàlisi del procés actual i el Desenvolupament i Millora del Procés.

La dedicació i les hores estan ben definides i detallades fent un total de 0,26 FTE. El dimensionament del conjunt del servei és correcte, superant fins i tot les hores demanades en el plec.

La proposta presenta una identificació dels recursos clara així com la descripció de les funcions de cada perfil i la dedicació què tindran. El dimensionament del conjunt del servei és correcte, superant fins i tot les hores demanades en el plec.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.6 S2Grupo

### A: Solució proposada (fins a 3 punts)

Els procediments associats són correctes, estan molt ben estructurats i abasten tots els aspectes relacionats amb la gestió de les vulnerabilitats. Tots els procediments cobreixen amb escreix les activitats detallades en el plec. Les fases queden cobertes perfectament amb l'explicació proposada pel licitador en el procediments i la metodologia aplicada. Això fa que quedin del tot cobertes les necessitats demanades en el plec.

El licitador proposa l'ús d'un conjunt molt ampli d'eines basades tant en codi obert com eines de pagament. Això fa que sigui fàcilment replicable per la UOC en la seva pròpia infraestructura.

Les eines incloses a l'oferta són:Nmap, Nikto, Netstumbler, Tenable.IO, OpenVas, Acunetix, W3Af, Arachni, SonarQube, Mobile Security Framework (Mob-SF), Suite de intrusión Cobalt Strike, Metasploit Framework, Burp Suite, SQLmap, Ollydbg e IDAPro, Brutus o TCH Hydra, QuasarRAT, Shellter Pro y Veil, CMSMap, Wpscan, Joomlascan, Droopescan, AngularJS Batarang Chrome Extension, Htcap, OWASP AJAX, Crawling Tool, Paradox, Wafw00f o Imperva WAF detector, Wireshark, Aircrack-ng suite, Mdk, Hostapd y Hostapd-wpe, eines propies, Sysinternals suite, rundll32, regsvr32, powershell, IEExec, InstallUtil, msbuild, OpenDLP.

Les metodologies proposades s'ajusten perfectament a les requerides en el plec, s'utilitzaran metodologies reconegudes i avalades internacionalment. Utilitzaran també metodologia específica per a test d'intrusió complementant-ho amb tècniques pròpies de S2Grupo. Les metodologies que s'utilitzaran són: OSSTMM (Open Source Security Testing Methodology Manual) y OWASP (Open Web Application Security Project), així com la metodologia específica de test d'intrusió de GIAC Penetration Testing del SANS Institute.

No s'especifica directament cap calendari i es parla dins de la licitació d'una sèrie d'auditories "automatitzades" periòdiques, sense especificar les "no automatitzades". No s'ha evidenciat la presència citada de fites.

La proposta és molt completa i descriptiva en alguns àmbits. La descripció que es fa és en algun moment extremadament prolixa però s'ha trobat a faltar la presència d'un calendari que faci una previsió de les activitats amb una temporalitat real associada. Tanmateix no s'han trobat les fites que haurà d'assolir el servei. Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els recursos estan correctament identificats en un organigrama que presenta el licitant. Cadascun del perfils té uns rols associats i es detalla la dedicació en hores de cadascun d'aquests perfils de forma suficientment per la dedicació en particular a l'activitat. El dimensionament del conjunt del servei és correcte.

Es defineix un perfil de tècnic especialista en hacking ètic i pentesting. S'associen 3 rols diferents per a aquest perfil, un d'ells és expert en gestió de vulnerabilitats, que es el que correspondria a aquest servei en concret. No obstant, les funcions i tasques no queden definides dins l'oferta.

La proposta presenta una identificació correcta dels recursos, així com la dedicació que aquests perfils duran a terme. El dimensionament del conjunt del servei és correcte, tot i això les funcions no estan definides. Per tot el que s'ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.

La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.7 S21Sec

### A: Solució proposada (fins a 3 punts)

El licitador fa una descripció molt superficial del servei, citant únicament les tasques principals però sense entrar en el detall de les mateixes, no es desenvolupen. També es fa menció a què els els "administradors" poden configurar-se els escanejos segons una sèrie de criteris però no explica quins són aquests administradors ni on ho configuren.

Els procediments associats malgrat que són correctes no s'ajusten del tot als requeriments de la UOC perquè la descripció dels mateixos no correspon a les activitats citades en el plec. les fases definides en el plec són les següents: Planificació i execució de l'anàlisi de vulnerabilitats, avaluació i validació de resultats, notificació de resultats per al seu seguiment.

Els apartats que no s´han inclòs en aquesta proposta i que eren objecte de valoració són: eines o mitjans, metodologies, calendari, ni fites.

Tenint en compte això, es considera que la proposta no permet assolir d´una forma completa i detallada els requeriments funcionals i tecnològics indicats en el plec.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta presenta un recurs que es tracta d'un operador de nivell 1, aquest perfil no s'identifica amb el servei amb les funcions que es mencionen, només parla de "recursos del departament d'auditories en funció del tipus d'escaneig". Les funcions del personal assignat no són atribuïbles a aquest servei, ni les acreditacions que es demanaven per aquestes persones. El dimensionament del conjunt del servei és el mateix que demana la UOC en el plec.

La oferta del proveïdor detalla el següent:

- Perfil: Operador/nivell 1
- Funcions:
    - Recepció d'incidències
    - Execució de procediments
    - Escalat d'incidències
    - Monitorització d'elements de seguretat
    - Analitzar, verificar i comprovar les incidències.

- Promig de 3 escanejos a l'any. Dedicació de 240 hores / any.

La proposta presenta una identificació molt abstracta dels recursos així com de les funcions i dedicació d'aquests que no ha pogut ser determinada en el plec. El dimensionament del conjunt del servei és el que es demana en el plec. Les funcions detallades no corresponen amb les que es demanen per a aquest servei, són funcions genèriques i més pròpies per a resolució d'incidents.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.8 SAYTEL SERVICIOS INFORMÁTICOS

### A: Solució proposada (fins a 3 punts)

Els procediments associats són correctes i les fases associades estan molt ben definides i de forma extensa. Cada fase presenta les tasques a realitzar associades. Les fases estan explicades correctament, amb les activitats lligades a cada fase. Es detallen les fases següents: Fase de Definició, Fase d'Execució, Fase de Presentació de resultats.

El licitador proposa l'ús d'un conjunt molt ampli d'eines basades tant en codi obert com eines de pagament. Això fa que sigui fàcilment replicable per la UOC en la seva pròpia infraestructura. Les eines són les següents: Sistema d'escàner de vulnerabilitats Nessus Professional, Distribució GPL Kali Linux que inclou: Framework Mestaploit: Explotació de Sistemes Operatius, Paquet BurpSuite: Detecció de vulnerabilitats a aplicacions web, Cercadors especialitzats: Shodan, NameCHK, Knowem, Tineye, etc., Eines de recol·lecció de metadades: Metagoofil, Libextractor, Eines RRSS: OsintStalker, Cree.py, Theharvester, Maltego.

Es menciona que s'utilitzaran les metodologies estàndards per anàlisis de vulnerabilitats concretament Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF) i Open Web Application Security Project (OWASP). Per tant, es dóna resposta al que especifica el plec.

Es proposa un calendari d'execució de les activitats per a aquest servei. També hi ha un calendari de fites, encara que no està gaire explicat. En tot cas, dóna resposta al plec.

El licitador fa una bona descripció del serveis i de forma molt directa i entenible explica cadascun dels punts demanats en la valoració d'aquest plec. No entra en massa detall especialment en la part de metodologia i fites però el contingut general és correcte i s'ajusta a les necessitats de la UOC.

Per tot el que s'ha exposat, la proposta es considera apropiada ja que dóna resposta a tot el que es demana en el plec, es considera que la proposta cobreix tots i cadascun dels punts exigits en el plec.

**3 punts**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Les tasques de cada perfil estan ben identificades i segregades en relació al recurs assignat i al servei.

El dimensionament està expressat en percentatges respecte unes "hores estimades" que s'entén són les que marca el plec.

La proposta inclou els perfils necessaris pel servei:

- Tècnic especialista en hacking ètic i pentesting (80% dedicació sobre el total d'hores estimades):
    - Tasques de configuració de eines de escaneig, explotació i cerca d'informació a internet.
    - Llançament de test semi automatitzats.
    - Explotació de vulnerabilitat per a reducció de falsos positius
    - Anàlisis de vulnerabilitats per depuració del llistat.
- Auditor en seguretat de la informació i continuïtat de negoci (12% dedicació sobre el total d'hores estimades):
    - Anàlisis de vulnerabilitats per depuració del llistat.
    - Elaboració d'anàlisi de risc.
    - Classificació de vulnerabilitats per criticitat i impacte.
    - Estudi d'impacte CID (Confidencialitat, Integritat i Disponibilitat).
- Professional certificat en seguretat de la informació. (8% dedicació sobre el total d'hores estimades):
    - Anàlisis de vulnerabilitats per depuració del llistat.
    - Realització d'informe amb les contramesures.
    - Informe sobre projectes que suposin punts de millora per a la reducció del factor d'exposició dels serveis, plataformes e infraestructures.

Els perfils dels recursos assignats pel licitant estan ben definits. Les activitats per les funcions de cada perfil estan ben especificades i són molt coherents amb les fases.

Per tot el que s'ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s'inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.

Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.1.9 T-Systems

### A: Solució proposada (fins a 3 punts)

T-Systems fa una proposta basada en l'ús d'una eina propietària anomenada VUMES i probablement adaptada pel licitador en mode SaaS. D'aquesta eina no s'especifica cap funcionalitat de forma detallada referent a:

- les pròpies funcionalitats de la eina
- les adaptacions de la mateixa que n'ha fet T-Systems

La proposta no contempla l´ús d eines en codi lliure o que puguin ser usades fora de l´entorn del licitador.

Tanmateix el servei es  recolza en un altre servei d'alerta primerenca del seu SOC però no explica la integració d'aquest servei amb la UOC especialment d'aquelles vulnerabilitats susceptibles d'afectar pròpiament la infraestructura de la UOC.

Els procediments associats són correctes i estan descrits dins de cadascuna de les fases del servei. Malgrat que el licitador especifica una sèrie de fases associades al servei aquestes no estan representades en cap calendari i per tant la UOC no pot conèixer la seva temporalitat. Les fases descrites en l'oferta són: Identificació, detecció, normalització, anàlisi del risc, mitigació i verificació.

El licitador només cita l'ús de la eina VUMES que és propietària i de desenvolupament propi del mateix. No compleix les expectatives UOC ja que no permet esbrinar cap de les funcionalitats de la mateixa eina.

No s'ha pogut trobar en la descripció del servei cap metodologia associada al mateix descrita pel licitador, així com tampoc s´ha inclòs ni el calendari ni les fites a assolir.

La proposta es considera poc apropiada per la UOC ja que no contempla un calendari ni fites al servei.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta enumera els recursos que s'assignaran al servei:

- Customer Security Manager (CuSM),  amb un rol en el servei de coordinador , una dedicació del 10% i les següents funcions: coordinació, comunicació, seguiment, informes, reunions.
- Analista N2, amb un rol de tècnic especialista hacking, una dedicació del 70% i les següents funcions: anàlisi de vulnerabilitats, documentació, operació, mesures correctores.

- Analista N1 amb un rol d´auditor de seguretat, amb una dedicació del 10% i les següents funcions: auditories i informes.
- Analista N1, amb un rol de professional certificat, una dedicació del 10% i les següents funcions: anàlisis de riscos, informes, seguiment SGSI

Les tasques de cada perfil s´han definit de forma molt genèrica i incompleta (ex: una de les funcions del coordinador del servei és la de “Coordinació”, però no especifica si és una coordinació interna, o entre T-Systems i la UOC). El dimensionament de quatre recursos pel servei és molt correcte

La proposta presenta una identificació dels recursos que no és suficientment satisfactori per la UOC i tanmateix parla d'alguns recursos de forma molt generalista i en alguns casos assignant-los tasques que no pertanyen al servei en qüestió, com per exemple, l’anàlisi de riscos.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

# 1.2. Gestió i resposta a incidents de seguretat de la informació CSIRT (fins a 6 punts)

## 1.2.1. ERNST & YOUNG Global Limited

### A: Solució proposada (fins a 3 punts)

Els procediments associats són correctes, coherents amb l'especificat al plec i s'adapten al que es demana per la UOC d'aquest servei. Aquests procediments consten de 3 etapes, preparació, resposta i recuperació. Cadascuna d´elles té associades diferents sub-fases i tasques.

El licitador cita l'ús d'eines bàsicament de seguiment que tot i ser suficients es podrien complementar amb alguna altra eina més. Les eines que cita són: SIEM, JIRA, OneTrust, CMDB / SCCM / etc, eines de protecció i perímetre (per ex. IPS).

Les metodologies proposades compleixen perfectament amb el que es demanava en el plec. Es basa en les guies CCN-STIC-403 i CCN-STIC-817. EY proposa millores als processos a valorar per la UOC segons el seu EY Cyber Incident Response Framework. Un marc de treball basat en la metodologia NIST SP.800-61 - Computer Security Incident Handling Guide.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari, tot i així el licitant especifica les fites a assolir en el calendari anual bàsicament per procedimentar.

Les fases són totalment coherents i satisfactòries per la UOC en relació al plec. La llista d'aquestes, sense entrar en detall, és: Recopilació de la tota la informació i Anàlisi de l'incident, Fase de Contenció, Eradicació i Recuperació de l'incident i Fase de Post-Incident..

Les fites senyalades són perfectament coherents. En resum són: Connexió EY Cybersecurity Operations Center, Accessos a eines de la UOC i Requeriments per respondre a incidents (per exemple al JIRA o SIEM), Auditoria de l'estat de les eines i els processos, així com els fluxes de treball i matrius d'escalat per grups,  Definició del procés i el service manual, establint fluxes, eines i matrius pel funcionament del servei gestionat, Posada en marxa servei CSIRT de manera parcial, per donar resposta a necessitats de la UOC, Posada en marxa servei CSIRT de manera total, Escaneig / auditoria sota demanda o específica de recheck i Pla d'evolució trimestral i seguiment de les accions d'evolució executades.

Ernst & Young fa una proposta correcta, metòdica, estructurada i comprensible, que s'adapta a les necessitats de la UOC expressades en el plec de prescripcions tècniques.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
    - El procediment que seguirà el proveïdor per gestionar-la
    - Els mitjans que s´utilitzaran
    - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils estan molt ben definits. Hi ha un perfil específic de "Especialista" en resposta a incidents de seguretat de la informació. Aquests perfils es componen de:

- COORDINADOR DEL SERVEI DE SEGURETAT amb les funcions de: Realitzar el seguiment del servei continuat i de les activitats que poden ser peticionades de manera discreta. Seguir i gestionar possibles desviacions de la planificació i pressupost. Coordinar el compliment de calendaris, fites, superació de barreres i implicació dels actors involucrats. Consolidar i aportar iniciatives que permetin la presa de decisions operatives i estratègiques. Realitzar el reporting del servei. Donar suport a la realització / verificació d'estimacions de nous serveis dins del manteniment evolutiu. Gestionar adequadament la demanda del servei per tal d'assegurar l'adaptabilitat i la màxima qualitat.

-TÈCNIC ESPECIALISTA EN RESPOSTA A INCIDENTS DE SEGURETAT DE LA INFORMACIÓ amb les funcions de: Recopilació, classificació, etiquetat i registre de tota la informació associada a l'incident. Lideratge, anàlisi, i definició de la línia d'actuació per afrontar l'incident. Suport i assistència a comitè de crisi i reunions que es derivin de la gestió de l'incident. Participació en processos dins l'àmbit legal, cadena de custòdia d'evidències, defensa del cas, etc. Definició, seguiment i reporting de les accions in situ de contenció, mitigació i eradicació de l'incident. Participació en la gestió d'evidències, des de la seva obtenció, anàlisi i preservació. Redacció i/o suport en la generació de lliurables de seguiment, tècnics i executius. Propostes de millora, anàlisi i definició de processos de gestió, resolució de problemàtiques. Revisió, definició i creació de procediments i instruccions operatives. Relació amb tercers per la resolució d'un incident.

-AUDITOR DE SEGURETAT DE LA INFORMACIÓ amb les següents funcions: Suport a l'auditoria inicial a realitzar com a primera fase del servei de seguretat gestionada. Executar i coordinar els projectes d'auditoria tant de marc normatiu com de compliment legal (evolució i millora). Documentar i presentar els resultats de les auditories d'acord amb el sistema i metodologia de valoració i de reportat establert. Incorporar i mantenir la informació de les auditories a OneTrust..

- PROFESSIONAL CERTIFICAT EN SEGURETAT DE LA INFORMACIÓ per al: Suport en la definició, transformació, industrialització i formalització organitzativa de les diferents tasques del servei de seguretat gestionada. Suport en la definició, evolució, desplegament i seguiment d'un model de gestió de la seguretat de la informació per la UOC. Identificació d'oportunitats de millora i riscos en la gestió de seguretat en base a millors pràctiques. Execució de projectes de seguretat de la informació en l'àmbit de la consultoria. Suport a tasques de realització de quadres de comandament.

La dedicació i les hores estan ben detallades fent un total de 520 hores anuals. Juntament amb la dedicació del coordinador del servei i de l'auditor (236 hores/any) fa que el dimensionament sigui correcte i suficient.

La proposta presenta una identificació dels recursos molt ben detallada. Els perfils estan clarament identificats, així com les funcions que realitzarà. Es millora considerablement el número d'hores proposades per perfil.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s'inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

### 1.2.2. Viewnext

#### A: Solució proposada (fins a 3 punts)

El licitador Viewnext fa una proposta correcta, molt canònica, en ocasions massa prolixa, que en general s'aparta del que es demana en la licitació però que podria adaptar-se a les necessitats de la UOC encara que de una forma basada en l'ús absolut dels serveis d'un SOC i unes infraestructures gestionades. La UOC no proposava l'adopció d'un SOC i la seva filosofia, com a solució al servei de gestió i resposta d'incidents, encara que sí ho faria a que el servei es prestés des d'un d'aquests centres.

Els procediments associats són absolutament correctes, ja que tota la oferta està basada en la metodologia del CCN-CERT dins del marc de l'ENS tal i com es demanava en el plec.

El licitador cita l'ús de les eines especificades en el plec però no en proposa cap d'específica ni llista les possibles eines que utilitzarà o que quedarien a disposició de la UOC. Únicament cita com a eines de comunicació les que la pròpia UOC facilita als seus proveïdors i que estaven escrites en el plec: Atlassian JIRA i OneTrust.

Les metodologies proposades pel licitador compleixen perfectament amb el que es demanava en el plec. I es basen en l'ús de les guies CCN-CERT dins del marc de l'Esquema Nacional de Seguretat (ENS), desenvolupades en les guies CCN-STIC-403 i la CCN-STIC-817.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. El licitador explica que el servei és proporcionat pel SOC de Madrid en horari 24x7 però no explica com ho farà per ser-hi en les dependències UOC tal i com es demana en el plec.

Les fases són totalment coherents i satisfactòries per la UOC en relació al plec i la metodologia proposada. Es poden resumir en: Identificació, Anàlisi i triatge, Contenció i mitigació i Eradicació.

No s'han pogut trobar fites assignables en la oferta relatives al servei de Resposta a Incidents de Seguretat.

La proposta descriu bé totes les fases i la metodologia a utilitzar. Queda el dubte raonable de com el licitant pensa donar sortida als temps de resposta i als temps d'intervenció a les dependències UOC al parlar només del SOC a Madrid.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils i les seves responsabilitats estan ben definits i són molt extensos, arribant-se a definir fins a 6 perfils per aquest servei.

Les hores de dedicació no estan ben definides i es troba a faltar una imputació d'aquestes als recursos.

El dimensionament és correcte, tot i que , es troba a faltar una relació directa entre la UOC i el gestor del servei licitat del proveïdor.

La proposta presenta una identificació dels recursos i les seves responsabilitats molt detallada. Els perfils estan clarament identificats, així com les funcions que realitzarà. En el model de relació que s'oferta es troba molt a faltar la relació directa entre la UOC i el responsable del servei per part del proveïdor, acabant-se aquesta relació en el denominat Nivell 2 de Triatge.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.3. IThink UPC

### A: Solució proposada (fins a 3 punts)

Els procediments associats són absolutament correctes, i basats en la metodologia del CCN-CERT dins del marc de l'ENS tal i com es demanava en el plec. La descripció que es fa dels mateixos és del tot correcta i satisfactòria per la UOC. La llista de procediments ofertats inclou: Documentar accions realitzades, les evidències recol·lectades, les conversacions i les dades subministrades per persones relacionades amb l'incident (usuaris, administradors, etc…). Identificació de l'incident amb un anàlisi de l'evidència inicial per confirmar que es tracta d'un incident i descartar un fals positiu. Notificació de l'incident als responsables dins de la UOC donant només la mínima informació necessària per evitar fuita d'informació. Notificació al CCN-CERT si s'escau. Aplicar mesures de Contenció. Anàlisi i Investigació. Solució i recuperació. Confirmar que la situació ha tornat a la normalitat. Contactar amb les forces i cossos de l'estat si es detecta activitat il·lícita. Procés de Reflexió i millora.

Els mitjans i les eines a utilitzar en cas d'incident citats són molt amplis i perfectament assumibles per la UOC. Tanmateix es proposa alguna millora al que s'havia especificat en el plec. En general a banda de les pròpies de la UOC com JIRA i OneTrust, el licitador proposa l'ús de: GHIDRA, IDA, RADARE, ENCASE, NESSUS i ACUNETIX.

Les metodologies proposades compleixen perfectament amb el que es demanava en el plec i són coherents amb els procediments abans explicats. Es cita: se seguirà la metodologia de la guia CCN-STIC-403 complementada amb aspectes de les guies CCN-STIC-817 y NIST.SP.800-61r2.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. Explica de forma correcta com donar servei als possibles incidents i com assistiran in situ en cas de necessitat en el temps acordat al plec.

Les fases són totalment coherents i s´ajusten al que es requereix  al plec i la metodologia proposada. Corresponen en aquest cas al mateixos procediments explicats: Preparació i prevenció, Detecció i identificació, Notificació, Contenció, Anàlisi i Investigació, Solució i Recuperació i Reflexió i Millora.

Les fites són correctes. Encara que s'ha trobat a faltar una mica de detall en relació a les possibles bretxes de seguretat amb afectació a dades personals es valora molt positivament que es facin enquestes de satisfacció al client posteriorment a la finalització de l'incident.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
    - El procediment que seguirà el proveïdor per gestionar-la
    - Els mitjans que s´utilitzaran
    - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils, les seves funcions i les assignacions estan definits.

Les funcions que descriu el licitador per aquest servei es poden resumir en:

- Un Coordinador del servei amb les funcions de seguiment del servei i de gestió de la demanda. També en funcions d'interlocució i planificació. Així com vetllar per l'aprovisionament correcte del servei més el seguiment.

- Quatre especialistes de seguretat amb funcions de: Suport legal, Infeccions per malware en general, Atacs d'invasió, DDoS, Defacement, Phising, Hacking, Frau utilitzant mitjans tecnològics, Violació de les polítiques de seguretat, Intrussions en servidors o punts de treball, Fuita de dades / fuita d'informació confidencial, Ransomware en punts de treball i servidors, Monitoratge de logs, Altres incidents, Redactar informes executius, Emetre recomanacions sobre noves vulnerabilitats i amenaces i Documentar el procés de resposta d'incidents.

Les hores de dedicació són correctes i es proposa un plus sobre el plec fent un total de 480 + 72 hores anuals. Les funcions i el dimensionament estan ben determinades per les fases i procediments descrits abans i són satisfactoris.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s'inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.4. (UTE) Opentrends + Cybernforce + Proficio

### A: Solució proposada (fins a 3 punts)

El proveïdor basa tota el seu plantejament de servei en l'ús d'una plataforma anomenada "ProSOC" com un servei que es tipifica en la oferta com a "SOC-as-a-Service". D'aquesta plataforma no s'explica gairebé res de les seves funcionalitats i tampoc s'explica com dóna resposta als punts de la valoració del plec.

No s'han trobat procediments escrits en la oferta relatius als descrits en el plec per aquest servei.

No es mencionen les eines que es sol·licitava ni tampoc cap eina estàndard de mercat. Únicament fa referència a una eina ProSOC de la que no s'especifica tècnicament el que fa amb detall.

No s'han trobat citades les metodologies demanades per poder gestionar aquest servei.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. Per tant no es valora negativament que no hi sigui.

No s'ha pogut trobar cap llista o descripció de les fases que ha de tenir el servei, explicades en la oferta del licitador.

No s'han pogut trobar fites associades a la prestació del servei.

En general parla de la implantació d'una eina anomenada ProSOC de la què es pot deduir, encara que no assegurar, que es tracta d'un SIEM en les dependències del proveïdor. Cosa que s'aparta de les especificacions del plec.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta del licitador no s'identifiquen els recursos assignats, ni descriu la dedicació i funcions de cada un dels perfil, per tant, tampoc es pot avaluar el correcte dimensionament dels recursos.

- **0 punts**: La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

## 1.2.5. PricewaterhouseCoopers PwC

### A: Solució proposada (fins a 3 punts)

Els procediments són correctes i la proposta que en fa el licitant és prou satisfactòria per la UOC. Es valora positivament la piràmide de procediments i objectius proposada per la posta en funcionament d'aquest servei. Al estar basats principalment en CCN-STIC-817 se superposen a les fases de la prestació del servei. En resum són i de forma iterativa: Preparació, Identificació, Resposta, Recuperació i Seguiment.

Les eines proposades corresponen a les demanades en el plec i és basen en l'ús de JIRA i OneTrust.

Les metodologies a aplicar són coherents, variades i d'acord amb el que es demanava en el plec. Inclouen: les guies del CCN-CERT, el US-CERT, NIST.SP.800-61(r2), CERT Societe Generale, CCN-STIC-817 o les FIRST-BPGL.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. Hi ha una sèrie de fites sobre la millora del procediment que queden ben marcades en el calendari.

Les fases del servei queden ben definides i es pot considerar que compleixen amb escreix el demanat al plec. S'ha trobat a faltar, no obstant, algun tipus de fase o resposta especial per les bretxes de seguretat amb afectació a dades de caràcter personal. No obstant és molt valorable que categoritzin els incidents en la línia del plec de la UOC i que per respondre a incidents crítics s'assisteixi en la creació de procediments operatius de resposta, què caldrà fer.

Les fites són perfectament coherents amb les fases. No són massa extenses ui es resumeixen en: Anàlisi dels processos actuals, Desenvolupament i millora del procés i Actuacions.

La descripció de la proposta és completa i detallada. Es descriuen les diferents fases del servei. També hi ha un calendari de fites. S'ha valorat positivament que es plantegés la creació dels procediments associats al servei com una fita.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Les activitats per les funcions de cada perfil, estan definides:

- Perfil especialista en resposta a incidents de seguretat de la informació
- Perfil auditor en seguretat de la informació i continuïtat de negoci
- Perfil certificat en seguretat de la informació
- Coordinador del servei

La seva dedicació al servei està definida i les hores són considerades més que suficients superant amb escreix el demanat per la UOC. Aquestes funcions en general es poden resumir com: Anàlisi del procés actual, Desenvolupament i millora del procés, Suport expert a les situacions que ho requereixin, Coordinació del servei.

El dimensionament de l'equip i dels perfils assignats al servei, 5 en total, és correcte i satisfactori. Les hores totals que proporcionaria el licitador són 0,55 FTE més hores sota demanda en cas de necessitat d'experts.

La proposta de recursos és bona, correspon als criteris de valoració demanats i s'adapta al servei.. Encara que no ho cita explícitament fa referència a una adhesió total als criteris de nivell de servei demanats al plec i per tant s'hauria de sobre-entendre la presència in-situ del servei a la UOC en cas de necessitat.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.6. S2Grupo

### A: Solució proposada (fins a 3 punts)

Els procediments són correctes i molt detallats. De vegades massa i tot el que provoca que vagi en detriment a l'espai que s'hauria pogut dedicar a explicar d'altres serveis. Les fases del servei queden ben definides i es pot considerar que compleixen amb escreix el demanat al plec. S'ha trobat a faltar, no obstant, algun tipus de fase o resposta especial per les bretxes de seguretat de cara a les agències de protecció de dades. Les fases descrites en aquest servei són: Preparació, Detecció, Resposta, Informes.

Les eines proposades són correctes encara que no en mencionen cap de les especificades en el plec.

Les metodologies a aplicar són coherents i d'acord amb el que es demanava en el plec. Com poden ser el SANS Institute o el NIST a la seva guía Guide to Integrating Forensic Techniques into Incident Response Special Publication 800-86.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. No s'ha pogut trobar, no obstant, cap calendari amb fites associades al servei.

La descripció de la proposta és completa i massa detallada. Aquest fet, la manca de concreció i l'excessiu detall, ha anat en detriment de la descripció més acurada de d'altres serveis.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils dels recursos assignats pel licitant són correctes i estan definits sense massa detall. Les activitats per les funcions de cada perfil no estan definides i només es cita el seu rol dins del servei. La seva dedicació al servei està definida i les hores es poden considerar suficients pel què és demanat per la UOC. No queda ben definit quin és el dimensionament de l'equip assignat al servei de resposta a incidents.

El perfil que exposa l'oferta per a aquest servei és Tècnic especialista en resposta a incidents de seguretat de la informació. Les hores dedicades per a aquest perfil estan barrejades amb d'altres perfils, el que no ens permet discernir una dedicació clara.

No hi ha una descripció detallada dels perfils assignats a aquest servei. Es troba a faltar una millor descripció de les activitats de cadascun dels perfils citats en la oferta pel rol que té dins del servei.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.7. S21Sec

### A: Solució proposada (fins a 3 punts)

S21Sec fa una descripció parcial del servei demanat per la UOC, ja que només descriu un servei de DFIR (un cas particular del servei de gestió d'incidents, quan aquests són considerats crítics) i per tant s'adequa només en part al demanat en el plec. Tanmateix el licitador fa referència a serveis de custòdia que en el cas de necessitar-se afirma que hauria de ser la UOC la qui es fes càrrec de les despeses.

La proposta ha inclòs un gràfic on s'expliquen els procediments i el flux de treball d'una forma molt esquemàtica però aquests no estan descrits per tal que puguin ser valorats.

La oferta no descriu cap dels punts següents: eines o mitjans, metodologies, fases del servei. La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. No s'ha pogut trobar, no obstant, cap calendari amb fites associades al servei.

La descripció de la proposta és molt bàsica i parcial. Es troba a faltar una major adequació a les activitats i tipologies citades en el plec, així com els incidents no crítics. Cal destacar no obstant que la proposta cita els informes pel DPO i les agències de protecció de dades.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils i funcions que inclou la proposta són els següents:

- Perfil: Analista/Nivell 2
- Funcions:
    - Revisió y resolució d'incidents de seguretat escalat per Operacions
    - Gestió de dispositius de seguretat
    - Primer nivell de col·laboració amb l'equip de serveis Avançats de Ciberseguretat
- Perfil: Enginyer/Nivell 3 i Auditor/Analista forense
- Funcions:
    - Revisió y resolució d'incidents de seguretat escalat pel nivell 2
    - Gestió avançada de dispositius de seguretat
    - Nivell màxim de col·laboració amb l'equip de serveis Avançats de Ciberseguretat
    - Coordinació de l'equip de resposta a incidents
    - Creació d'informes, plans d'actuació i millora.

Volumetria: s'estimen 4 incidents al mes amb un promig de 14 crítics a l'any. Dedicació de 480 hores / any.

Els perfils definits son molt imprecisos i els recursos assignats són poc clars. No es detalla la dedicació de cada perfil a alguna activitat. Al no haver-hi la dedicació de cada perfil és impossible determinar si el dimensionament és correcte.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.8. SAYTEL SERVICIOS INFORMÁTICOS

### A: Solució proposada (fins a 3 punts)

El licitador SAYTEL SERVICIOS INFORMÁTICOS fa una proposta ben estructurada amb una sèrie de fases ben detalles i una molt bona referència a les notificacions a les agències de protecció de dades o a algun CERT en cas que la UOC hagués de complir l'ENS com a administració pública. Falta, no obstant, la descripció de la metodologia a usar i les fites del servei d'una forma explícita.

Els procediments són correctes i s'adapten al que s'especifica en el plec UOC pel servei. Les fases del servei queden prou ben definides i són satisfactòries per les necessitats de la UOC. Les fases descrites en l'oferta són les següents: Fase de preparació per la Resposta a Incidents, Fase d'identificació de l'incident, Fase de contenció, Fase d'eradicació, Fase de recuperació, Fase de Documentació Final i Conclusions.

Les eines citades fan referència bàsicament a procediments associats a l'anàlisi forense. Són les següents: Eina d'apertura de peticions SOLMAN, Eina de gestió documental: Microsoft SharePoint, Eines de recerca de Incidents de Ciberintel·ligència presents al SEIDOR SOC per a la detecció primerenca: Eines OSINT, Kit d'eines d'anàlisi forense Distribució Kali Linux: Binwalk, bulk-extractor, Capstone, chntpw, Cuckoo, dc3dd, ddrescue, DFF, diStorm3, Dumpzilla, extundelete, Foremost, Galleta, Guymager, iPhone Backup Analyzer, p0f, pdf-parser, pdfid, pdgmail, peepdf,RegRipper, Volatility, Xplico. També disposen de Memòries USB amb fitxers bootables, Eines de clonat Forense dispositius mòbils: Celebrity, Eines de clonat de disc dur: Tableu Forensic Duplicator, Lector de targetes, Càmera fotogràfica, Cables i adaptadors, Etiquetadora, Formularis d'adquisició.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. No s'ha pogut trobar, no obstant, cap calendari amb fites associades al servei. Tampoc hi ha cap metodologia citada explícitament.

La descripció especialment de les fases del servei és bona i entenedora a més de ben estructurada. Però no s'ha pogut trobar algun calendari amb les fites o activitats del projecte, malgrat que les fases de la solució proposada són correctes i s'adeqüen al servei. No hi ha fites del projecte ni calendari associat a les mateixes.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils dels recursos assignats pel licitant estan ben definits. Les activitats per les funcions de cada

perfil estan ben especificades i són molt coherents amb les fases. La dedicació al servei recau bàsicament i de forma molt majoritària només en un analista.

Els perfils exposats en l'oferta són els següents:

- Tècnic especialista en resposta a incidents de seguretat de la informació, especialitat analista software (90% dedicació sobre el total d'hores estimades):
    - Elaboració de llistat de comunicació per àrees.
    - Definició del pla o estratègia de resposta.
    - Definició del pla de comunicació.
    - Recopilació d'evidències.
    - Participar el en procés de notificacions de compliment normatiu.
    - Realització i coordinació de les tasques dins la fase de contenció de l'incident.
    - Realització i coordinació de les tasques dins la fase de contenció de l'incident.
    - Documentació durant tot el procés de l'incident.
    - Realització d'informes tècnics de conclusions.
- Auditor en seguretat de la informació i continuïtat de negoci (5% dedicació sobre el total d'hores estimades):
    - Anàlisi d'impacte de l'incident en el negocio de la UOC.
    - Revisió dels controls a política de seguretat.
    - Elaboració d'informes per a la comunicació a les entitats reguladores.
    - Proposta de millores en procediment o transacció per la qual s'ha rebut el incident.
    - Propostes de conscienciació o entrenament per usuaris.
- Professional certificat en seguretat de la informació. (5% dedicació sobre el total d'hores estimades):
    - Detecció i comunicació d'incidents de seguretat detectats en la monitorització de les plataformes de seguretat de la UOC.
    - Revisió d'indicadors clau de serveis i volumetries per establir llindars normals de funcionament.
    - Participació en la definició de proves durant la fase de recuperació.
    - Proposta de millores en els controls tècnics existents.

Malgrat que queda ben definit en la oferta del licitador, és possible que els percentatges de dedicació no quedin ben compensats entre tots els perfils.

Els perfils dels recursos assignats pel licitant estan ben definits. Les activitats per les funcions de cada perfil estan ben especificades i són molt coherents amb les fases. La dedicació al servei recau bàsicament i de forma molt majoritària en un analista

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.2.9. T-Systems

### A: Solució proposada (fins a 3 punts)

No es descriuen els procediments associats al servei que proposa el licitador. Les fases del servei no queden prou ben definides i en general només es parla de seguiment i informes de servei, i de les tipologies d'incidents a tractar.

Les metodologies proposades pel licitador estan basades en les guies STIC del CCN i són coherents amb el que es demanava en el plec.

La naturalesa d'un servei de CSIRT fa que no pugui estar lligada a un calendari. No s'ha pogut trobar, no obstant, cap calendari amb fites associades al servei.

No s'ha pogut trobar cap llista d'eines per poder donar suport al servei, ni les fites associades al servei.

T-Systems fa una proposta molt centrada en el seu SOC de Madrid i en fa una descripció molt detallada del mateix. Parla d'una tipologia d'incidents alineada amb les guies CCN-STIC, cosa que s'alinea amb el demanat al plec de la UOC però no descriu procediments ni fases de la prestació del servei. Tampoc queda clar com es proporcionarà el servei in situ a la UOC.

No queda prou clar quin és el model de relació o els procediments organitzatius associats com a proposta del servei. És molt valorable, no obstant, que el licitador proposi una llista d'indicadors de servei per poder avaluar la qualitat del mateix.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils dels recursos assignats pel licitant no estan suficientment ben definits per poder-se valorar, ja que són molt genèrics. Les activitats per les funcions de cada perfil no estan prou ben especificades i no es poden assignar a cap fase o procediment. La dedicació al servei és correcte.

els perfils que inclou la proposta són:

- Customer Security Manager (CSUM). Aquest perfil tindrà un rol de coordinador de servei amb una dedicació del 20%. Les seves funcions són: coordinació, comunicació, seguiment, informes, reunions.
- Analista N2: Aquest perfil tindrà un rol de tècnic especialista Hacking, amb una dedicació del

30%. les seves funcions són: Anàlisi de vulnerabilitats, pentesting, documentació, operació.
- Auditor N1: Aquest perfil tindrà un rol d´Auditor de seguretat, amb una dedicació del 10%. Les seves funcions són: auditories, informes.
- Analista N1: Aquest perfil tindrà un rol de professional certificat amb una dedicació del 10%. Les seves funcions són: anàlisi de riscos, informes, seguiment SGSI.
- Analista N3: Aquest perfil tindrà un rol de tècnic especialista resposta, amb una dedicació del 40%. Les seves funcions són: anàlisi forense, malware, resposta a incidents.

Malgrat que hi ha un dimensionament correcte del servei, les funcions que tenen definides cadascun dels perfils no correspondrien amb el servei a prestar en aquest cas. es barregen funcions d'altres serveis, com poden ser les funcions d'anàlisi de vulnerabilitats o pentesting.

Per tot el que s'ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

# 1.3. Anàlisi de malware (fins a 6 punts)

## 1.3.1. ERNST & YOUNG Global Limited

### A: Solució proposada (fins a 3 punts)

La proposta inclou l'abast del servei i s'especifiquen els objectius a assolir. Fa una descripció de l'entorn de laboratori. Es detallen la metodologia i processos a seguir, incorporant un esquema.

Els procediments compleixen els objectius, i es fa una descripció en detall de les fases:

- Es definirà un procés conjuntament amb la UOC per la obtenció segura de les mostres de malware a tots els actius de la UOC, per a que puguin ser traslladats als Advanced Security Labs d'EY pel seu anàlisi. En aquest procés s'inclouran les instruccions operatives i eines necessàries / entorns per fer un anàlisi complet del malware.
- Avaluació, si és possible, l'aïllament de l'àmbit afectat i anàlisi del vector de la infecció per l'obtenció de la mostra a analitzar.

El licitador proposa les eines de EY Analysis Toolkit for static and dynamic malware analysis. Aquí s'inclouen un conjunt suficientment ampli d'eines què principalment són el EY Malware Analysis Toolkit for static and dynamic malware analysis: Entorns de laboratori virtuals i aïllats (Windows, Linux, Android, iOS), Eines de sandboxing, Eines d'anàlisi de comportament: Process Monitor, Process Hacker, Whireshark, Regshot, Eines d'anàlisi de codi: desensabladors, debuggers (OllyDbg, IDA Pro Freeware...), Bolcat de memoria (Scylla, OllyDumpEx...), Eines d'anàlisi online: Anubis, EUREKA, ThreatExpert, VirusTotal, WebInspector, … etc.

Es proposen dues metodologies per part de EY:

- Anàlisi agil + contenció
- Anàlisi profund + resposta

Les fases per a aquest servei estan correctament descrites i s'adeqüen al servei. Bàsicament corresponen a l'anàlisi del sistema, la fase d'anàlisi estàtic i la d'anàlisi dinàmic, cadascuna amb les seves corresponents sub-fases.

Tant el calendari com les fites es defineixen posteriorment en capítol apart.

La solució plantejada pel servei és completa, lògica, amb unes fases ben definides, una bona metodologia i unes eines molt adequades a la tasca. La solució proposada és coherent i la metodologia correcte. Les fases d'anàlisi d'una mostra de malware estan molt ben definides i estructurades. La descripció de les diferents fases i els resultats de les mateixes són adequats al que es demana en el plec.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
    - El procediment que seguirà el proveïdor per gestionar-la

- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils estan clarament identificats en un capítol apart, així com les funcions. Aquests perfils es composen de:

-COORDINADOR DEL SERVEI DE SEGURETAT amb les funcions de: Realitzar el seguiment del servei continuat i de les activitats que poden ser peticionades de manera discreta. Seguir i gestionar possibles desviacions de la planificació i pressupost. Coordinar el compliment de calendaris, fites, superació de barreres i implicació dels actors involucrats. Consolidar i aportar iniciatives que permetin la presa de decisions operatives i estratègiques. Realitzar el reporting del servei. Donar suport a la realització / verificació d'estimacions de nous serveis dins del manteniment evolutiu. Gestionar adequadament la demanda del servei per tal d'assegurar l'adaptabilitat i la màxima qualitat.

-TÈCNIC ANÀLISI DE MALWARE amb les funcions de: Realitzar una anàlisi de malware sobre mostres de deteccions malicioses localitzades o incidents registrats en els equips de la infraestructura de la UOC. Conèixer el comportament i possible origen del malware que rep la UOC amb la finalitat de dissenyar una resposta (per exemple regles YARA) de prevenció i protecció així com investigar incidents i/o analitzar presumptes fugides d'informació o altres esdeveniments que haguessin pogut afectar la confidencialitat, integritat i disponibilitat. Conèixer el perfil de ciberamenaça i comunicar els resultats en un llenguatge comprensible.

-AUDITOR DE SEGURETAT DE LA INFORMACIÓ amb les següents funcions: Suport a l'auditoria inicial a realitzar com a primera fase del servei de seguretat gestionada. Executar i coordinar els projectes d'auditoria tant de marc normatiu com de compliment legal (evolució i millora). Documentar i presentar els resultats de les auditories d'acord amb el sistema i metodologia de valoració i de reportat establert. Incorporar i mantenir la informació de les auditories a OneTrust..

- I un PROFESSIONAL CERTIFICAT EN SEGURETAT DE LA INFORMACIÓ per al: Suport en la definició, transformació, industrialització i formalització organitzativa de les diferents tasques del servei de seguretat gestionada. Suport en la definició, evolució, desplegament i seguiment d'un model de gestió de la seguretat de la informació per la UOC. Identificació d'oportunitats de millora i riscos en la gestió de seguretat en base a millors pràctiques. Execució de projectes de seguretat de la informació en l'àmbit de la consultoria. Suport a tasques de realització de quadres de comandament.

El dimensionament és el demanat, inclús incrementant el nombre d'hores. ja que el tècnic de malware es dimensiona amb 80 hores i el Consultor de seguretat amb 20 hores.

ERNST & YOUNG Global Limited fa una descripció molt detallada de cada perfil situant-lo dins una estructura organitzativa on podem observar el dimensionament global del servei a prestar.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als

criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.2. Viewnext

### A: Solució proposada (fins a 3 punts)

El licitador descriu a la seva oferta el fet de proporcionar a la UOC la capacitat d'analitzar i comprendre el funcionament de codi maliciós, però no exposa en cap moment com ho farà.

Els procediments associats a la prestació d'aquest servei no estan descrits.

El licitador tan sols menciona dues eines, una d'anàlisi de codi estàtic i l'altra de codi dinàmic que corresponen a: IDA Pro i OllyDBG.

Les possibles metodologies a utilitzar per l'estandarització del servei no estan descrites.

Donat que l'anàlisi de mostres de malware no és una activitat previsible, no hi hauria d'haver un calendari definit per l'activitat en sí. Podria ser-hi si s'associés a una metodologia. El calendari no està definit.

No s'han trobat llistades les fases per a aquest servei.

Les fites no estan descrites ni llistades.

La proposta presenta una definició molt poc clara i concisa. Hi ha una manca clara de contingut i no es defineixen fases, metodologia, procediments ni fites.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Es defineixen un perfil amb dues categories professionals. Corresponent a:

- Perfil: Tècnic especialista en hacking ètic i pentesting:
  - Categoria 1: Auditor expert en seguretat
  - Categoria 2: Analista de seguretat

Les funcions de les categories del perfil, per aquest servei a prestar d'anàlisi de malware, són:

-AUDITOR EXPERT EN SEGURETAT: Responsable de l'execució de les tasques, Seguiment de les mateixes, Responsable del seguiment operatiu, Responsable de la supervisió i coordinació, Realització dels informes , Preparació i presentació dels informes en les reunions, Anàlisi de millores i Garantir que les eines estan ben configurades i són les adequades.

-ANALISTA DE SEGURETAT: Elaborar i mantenir tota la documentació tècnica.

El dimensionament es el correcte. No cita les hores absolutes de dedicació, sinó que fa un percentatge del qual no indica la base a aplicar, per tant no permet conèixer el valor de les mateixes.

La descripció dels recursos és poc concisa. Les funcions encara que detallades, no tenen pràcticament res a veure amb el servei i les tasques a realitzar. Així per exemple es parla d'un perfil "TÈCNICO ESPECIALISTA EN HACKIN ÈTICO I PENTESTING" que no següent el perfil adequat per aquest servei de ANÀLISI DE MALWARE.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.3. IThink UPC

### A: Solució proposada (fins a 3 punts)

El licitador fa una proposta molt completa i coherent de la solució. Basa l'impacte d'una materialització d'una amenaça en la “Pyramid of pain” de David J Bianco i és una aproximació molt bona a l'ús de IOCs extrets de mostres de malware.

Els procediments compleixen els objectius, i es fa una descripció en detall de les fases. Aquests procediments són congruents amb la metodologia proposada i són: Prevenció i preparació, Detecció i Identificació, Notificació, Contenció, Anàlisi i Investigació, Solució i Recuperació, i Reflexió i Millora. Dins de la fase d'Anàlisi i Investigació, es seguirà el procediment CCN-STIC-912 d'Anàlisi i Recerca de Malware.

Es proposa un ventall ampli d'eines d'anàlisi de malware, com ara: Cuckoo sandbox, Whireshark, Ghidra, OllyDbg, x64dbg o gdb. La majoria d'elles en forma de programari lliure que s'adiuen perfectament a les necessitats de la UOC.

El licitador exposa que la metodologia de treball a usar està basada en CCN-STIC-912 d'investigació de codi nociu i la CCN-STGIC-403 per la resposta a incidents, en cas que fos necessari per la materialització de l'amenaça del malware. Aquestes dos metodologies proposades són plenament satisfactòries per la UOC.

L’anàlisi de malware és un servei sota demanda, per tant, no hi ha un calendari definit establert. Malgrat tot el licitador descriu perfectament una sèrie de fases i fites associades al servei.

Les fases per a aquest servei estan correctament descrites. Aquestes són: Desenvolupar el laboratori que s'utilitzarà per a l'anàlisi de malware. Configurar l’ús d’un servei de compartir fitxers que el client farà servir per compartir mostres de malware comprimides. Confirmar la presència de malware. Realitzar anàlisi dinàmica i/o anàlisi estàtica. Col·lecció d'IOCS. Compilar l'informe.

Les fites associades són molt correctes i es valora positivament que es realitzin enquestes de satisfacció: Mesurar la finalització de la fase preparatòria. Realitzar enquestes i qüestionaris de satisfacció al client després de cada anàlisi de malware. Revisió satisfactòria en el Comitè Estratègic i reflexió sobre possibles modificacions.

La solució aportada pel proveïdor està ben estructurada, és adequada a les necessitats exposades en el plec de la UOC, les fites estan ben dimensionades i les eines són àmplies i adequades. La solució aportada és correcta i coherent. La proposta d'implementació del procediment CCN-STIC-912 és correcte i s´adequa a les necessitats del servei.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Es defineix la dedicació i les funcions a realitzar de forma correcte. S'aporta el detall de dedicació de cada perfil: Vetllar per la provisió correcta del servei, Seguiment, Anàlisi d'artefactes Windows, Anàlisi d'artefactes Linux, Anàlisi d'artefactes Android, Anàlisi d'artefactes iOS, Redactar informes executius, Emetre recomanacions sobre noves vulnerabilitats i amenaces i Documentar el procés de resposta a malware.

Els perfils assignats pel licitador per aquest servei són:

- Un especialista en anàlisi de malware
- Un especialista en anàlisi forense
- Un professional certificat en seguretat
- Un auditor en seguretat i continuïtat de negoci
- Un coordinador del servei de seguretat
- Un gestor del servei

El dimensionament de l'equip compleix el requerit al punt 4.2.1.3 del plec tècnic i inclús supera en un 15% al volum demanant

IThink UPC ha creat una matriu corresponent a perfils i funcions assignades amb un percentatge de dedicació a cada funció. El dimensionament és el correcte.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.4. (UTE) Opentrends + Cybernforce + Proficio

### A: Solució proposada (fins a 3 punts)

La proposta presentada per (UTE) Opentrends + Cybernforce + Proficio consta d'una descripció molt superficial del servei i no entra en massa detalls.

Es defineix el procediment a dur a terme en 3 passos, però d'una forma molt superficial.

Tot i que no es menciona explícitament les eines que utilitzarà, la proposta fa referència a un mòdul de l´eina general Proficio, anomentat Proficio Threat Intelligence Profiler (TIP) que correspon a un servei de reputació.

Les metodologies no estan descrites en la oferta. L'anàlisi de malware és un servei sota demanda, per tant, no hi ha un calendari definit establert.la proposta no descriu ni les fases ni les fites.

La solució aportada en la oferta és pràcticament inexistent per aquest servei d'anàlisi de malware. Tot i que d´una manera molt superficial, la proposta defineix el procediment a dur a terme.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta del licitador no s'identifiquen els recursos assignats, ni descriu la dedicació i funcions de cada un dels perfil, per tant, tampoc es pot avaluar el correcte dimensionament dels recursos.

- **0 punts**: La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat

## 1.3.5. PricewaterhouseCoopers PwC

### A: Solució proposada (fins a 3 punts)

El licitador fa una proposta coherent de la solució aportada al servei. Proposa un enfoc metodològic respecte les peticions d'anàlisi de malware que es rebran en el servei.

Els procediments compleixen els objectius, i es fa una descripció en detall dins de cadascuna de les fases.

No s'ha trobat llistat les eines que proposa el licitador per a aquest servei.

No hi ha una metodologia clara basada en algun document o estàndard. En canvi proposa com a metodologia les pròpies fases del servei. Les fases per a aquest servei estan correctament descrites i són: Extracció i presa de contacte amb la realització d'un anàlisi forense i l'extracció del malware, Identificació i tipificació del malware, Anàlisi de comportament dinàmic, Anàlisi estàtic de la mostra de malware, Identificació i Elaboració d'informes o reporting.

L'anàlisi de malware és un servei sota demanda, per tant, no hi ha un calendari definit establert.. Les fites no estan descrites en la proposta.

La solució aportada pel proveïdor està ben detallada. No obstant, la proposta no contempla eines, metodologia ni fites.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els recursos plantejats pel licitador no queden clarament assignats i es parla només d'un Panell d´ Experts i Suport amb les funcions de: Anàlisi (Activitats d'anàlisi de malware sota demanda) i Reporting. Tots dos aspectes descrits de forma molt somera.

La descripció que es fa dels perfils i les seves funcions no estan descrites de forma correcta.

El dimensionament tenint en compte la manca de detall pel perfil i les funcions no es pot assegurar que sigui el requerit en el plec UOC.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.6. S2Grupo

### A: Solució proposada (fins a 3 punts)

La descripció està inclosa dins el servei de gestió d'incidents de seguretat d'una forma molt bàsica. Això invalida la possibilitat que la UOC aporti mostres possibles malicioses per la seva identificació i control si són fora d'un incident de seguretat

Es mencionen diferents eines com poden ser Cuckoo Sandbox, Ollydbg o x64dbg per a anàlisis dinàmic i eines de detecció de virus, detecció de patrons, com poden ser Yara, oletools per a Microsoft Office o peepdf per a fitxers de Adobe pdf.

No es defineixen en la oferta els punts següents: procediments, metodologia, calendari (tan sols s'indica que s'actuarà arrel d'un incident de seguretat), fases, ni fites.

La descripció està inclosa dins el servei de gestió d'incidents de seguretat d'una forma molt bàsica. Això invalida la possibilitat que la UOC aporti mostres possibles malicioses per la seva identificació i control si són fora d'un incident de seguretat

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Al final de la proposta s'identifiquen els diferents perfils d'una forma genèrica, però no hi ha definides les funcions clarament. Hi ha una definició per nivells 2 i 3, però no es relacionen amb els diferents perfils ni les tasques a executar.  El dimensionament és el requerit en el plec.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.7. S21Sec

### A: Solució proposada (fins a 3 punts)

El proveïdor fa una descripció correcte i coherent del servei que es demana, menciona diferents tipus d'anàlisi de malware que es podríen dur a terme, com poden ser: Automatic, Remote Analysis of Compromised Devices, Behaviour Analysis, Reverse Engineering of Malware.

Es detalla també el contingut dels entregables com a documentació. Es menciona que es farà servir la plataforma de compartició de malware : Malware Information Sharing Platform (MISP) per agregar informació d'altres clients.

En la oferta no es descriuen els punts següents: metodologia, fases del servei, ni fites. No es menciona calendari. Per a aquest servei seran peticions sota demanda

El proveïdor especifica una descripció detallada de la proposta tècnica. Però no s'expliquen fases, ni fites, ni metodologia.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Es descriu un únic perfil "Analista/Advanced Cybrsecurity Services". Es detalla la dedicació i les funcions d'un perfil molt genèric que entre d'altres funcions fa la de realitzar anàlisi sobre mostres malicioses. El dimensionament és el requerit en el plec.

Els perfil definit en l'oferta és el següent:

- Perfil: Analista / Advanced Cybersecurity Services (ACS)
- Funcions:
    - Revisió y resolució d'incidents de seguretat escalat pel nivell 2
    - Gestió avançada de dispositius de seguretat
    - Nivell màxim de col·laboració amb l'equip de serveis Avançats de Ciberseguretat
    - Coordinació de l'equip de resposta a incidents
    - Creació d'informes, plans d'actuació i millora.

Volumetria: s'estimen 5 anàlisis a l'any. Dedicació de 48 hores / any.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.8. SAYTEL SERVICIOS INFORMÁTICOS

### A: Solució proposada (fins a 3 punts)

Els procediments estan correctament descrits amb les fases que es demanen. Les fases per a aquest servei estan extensament descrites de forma adient a les necessitats del servei. Les fases definides són les següents: Fase de Comunicació, Fase d'anàlisi del Malware, Fase de presentació de resultats

Es descriuen les eines de les quals es composa el seu laboratori d'anàlisi de malware: Anàlisi automatitzat: Cuckoo Sandbox 2.0.7, Examen de les característiques del software: PeStudio 8.98, Examen del comportament del software: Linux REMnux, FLARE VM de Fireeye, Process Hacker, Process Monitor, Wireshark, OSINT, ProcDOT, Excel, Anàlisi Interacció amb Xarxa: WireShark, Linux REMnux, URLVoid, Generació de firmes: YARA.

El licitador no proposa cap metodologia per al servei. Tampoc es menciona cap calendari. Per a aquest servei seran peticions sota demanda. Les fites no estan descrites en la proposta.

La solució aportada pel proveïdor està ben estructurada, és adequada a les necessitats exposades en el plec de la UOC. No obstant, no presenta fites, no està basada en cap metodologia que citin en la oferta. Les fases de la solució són coherents i les eines usades són correctes i adequades. L'ordre en que es realitzen les tasques és coherent.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils presentats a l'oferta són els següents:

- Tècnic especialista en resposta a incidents de seguretat de la informació, especialitat analista software (90% dedicació sobre el total d'hores estimades):
    - Creació de peticions d'investigació, en el cas l'anàlisi de malware derivi d'un servei de resposta a incidents.
    - Parametrització de les eines del laboratori per a la anàlisis.
    - Tasques d'anàlisi automatitzat, estàtic, dinàmic i de xarxa.
    - Documentació i evidencia de les hipòtesis seguides en l'anàlisi.
    - Documentació de proves i resultats obtinguts.
- Auditor en seguretat de la informació i continuïtat de negoci (5% dedicació sobre el total d'hores estimades):
    - Anàlisi d'impacte de la infecció per malware en el entorn de la UOC.

    - Proposta de millores en procediment o transacció per la qual s'ha rebut el malware.
    - Propostes de conscienciació o entrenament per usuaris.
- Professional certificat en seguretat de la informació. (5% dedicació sobre el total d'hores estimades):
    - Anàlisi del comportament del malware vers els controls aplicats a les plataformes de protecció.
    - Proposta de millores en els controls existents.

La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats i les seves funcions.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.3.9. T-Systems

### A: Solució proposada (fins a 3 punts)

La proposta inclou una breu descripció de les 3 fases de les que es compon el servei, però aquestes no estan desenvolupades. Les fases mencionades en la oferta són: obtenció de l'artefacte a analitzar, l'anàlisi en si i l'informe de resultats. Els temps de resposta de la proposta són superiors als indicats en el plec de prescripcions tècniques.

No queden definits en l'oferta els procediments a seguir pel servei, les eines o mitjans, les metodologies, el calendari ni les fites.

La proposta còpia de forma literal el que s'especifica dins el PPT. No permet saber quina seria la proposta del licitador perquè no explica ni metodologies, ni descriu eines ni hi ha una explicació de les tasques o fases a realitzar. Dóna un temps de resposta de 7 dies, quan a la licitació s'indica un temps màxim de resposta de 2 dies.  No obstant, es mencionen les fases del servei.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

El licitador  indica 5 perfils dins d'aquest apartat, dels qual cap s'identifica clarament amb el servei a prestar. Es barregen els perfils dels altres serveis sense poder discernir quina dedicació i funcions es duran a terme per a aquest servei d'anàlisi de malware.

Els perfils que inclou la proposta són:

- Customer Security Manager amb un rol de coordinador del servei i una dedicació del 20%. Les seves funcions son: coordinació, comunicació, seguiment, informes, reunions.
- Analista N2 amb un rol de tècnic especialista hacking i una dedicació del 10%. Les seves funcions són: anàlisi de vulnerabilitats, pentesting, documentació, operació.
- Analista N1 amb un rol de professional certificat i una dedicació del 10%. Les seves funcions són: anàlisi de riscos, informes, seguiment SGSI.
- Analista N3 amb un rol de tècnic especialista resposta i una dedicació del 50%. Les seves funcions són Anàlisi forense, malware, resposta a incidents.

No hi ha una identificació gens clara del recurs contra el seu perfil. No es pot deduir a partir de les dades si el dimensionament és o no correcte.

La proposta presenta diferents perfils amb les seves funcions, però no s'identifiquen clarament amb el servei a prestar. No es pot deduir a partir de les dades si el dimensionament és o no correcte.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

# 1.4. Anàlisi forense (fins a 6 punts)

## 1.4.1. ERNST & YOUNG Global Limited

### A: Solució proposada (fins a 3 punts)

La proposta de ERNST & YOUNG Global Limited explica una descripció coherent del servei. Les fases estan ben descrites i corresponen a les necessitats de la UOC respecte al processament, recollida, control i emmagatzemament de les evidències electròniques i l'elaboració dels anàlisi forenses.

Els procediments compleixen els objectius, i es fa una descripció en detall de les fases. Aquests estan basats en un marc de treball de EY i són: Preliminary evidence assessment and identification, Collecting and securing the evidence, Image acquisition and validation, Examination and analysis i Executive summary and detailed report.

El licitador proposa les eines de EY Forensics Toolkit. Aquí s'inclouen un conjunt suficientment ampli d'eines. Aquestes eines ens permetran dur a terme anàlisis dinàmic i estàtic, així com d'altres. La llista de les eines proposades en la oferta és:

- Per a Data collection: Linux Live CDs, CaseFile, Dmitry, InTrace, Microsoft File Checksum Integrity Verifier.

- Per a Analysis: trID DFET Edition, Defraser, Localiza, Shadow Explorer, Foca / Forensic Foca, Forensic Image Viewer, Autopsy – The Sleuth Kit, Strings, libesedb to access the Extensible Storage Engine (ESE) Database File (EDB) format.

- EY Advanced Security Labs

La metodologia proposada forma part del marc de treball propi de EY. Aquesta metodologia inclou 17 Key Task incloses en el marc de treball, les quals permeten assolir els objectius d´una anàlisi forense.

El calendari està ben definit i les fites ben ajustades al mateix.

la proposta enumera i descriu de forma correcta les fases que tindrà el servei. Aquestes són: Fase d'avaluació i identificació d'evidències, Fase de recepció, categorització i adquisició, Fase d'imatge, validació i preservació, Fase d'examen, anàlisi i ampliació d'evidències i Fase de presentació de resultats, inventariat i arxiu / destrucció.

La proposta enumera i descriu de forma correcta les fites en el calendari. Aquestes són: Connexió EY Cybersecurity Operations Center, Accessos a eines de la UOC i Requeriments per anàlisi forense (accessos per exemple al JIRA o SIEM), Auditoria de l'estat de les eines i els processos, Definició del procés de l'anàlisi forense i el sistema de preservació d'evidències, Comunicació i formació dels processos a les parts interessades, Posada en marxa servei d'anàlisi forense de manera parcial, per donar resposta a necessitats de la UOC, Posada en marxa servei d'anàlisi forense de manera total, Pla d'evolució trimestral i seguiment de les accions d'evolució executades.

La proposta de ERNST & YOUNG Global Limited explica una descripció coherent. Les fases estan ben descrites i corresponen a les necessitats de la UOC respecte al processament, recollida, control i emmagatzemament de les evidències electròniques.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als

criteris que es valoren en aquest punt.

3 punts: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils estan molt ben definits. Hi ha un perfil específic de "Especialista" en resposta a incidents de seguretat de la informació. Aquests perfils es composen de:

- COORDINADOR DEL SERVEI DE SEGURETAT amb les funcions de: Realitzar el seguiment del servei continuat i de les activitats que poden ser peticionades de manera discreta. Seguir i gestionar possibles desviacions de la planificació i pressupost. Coordinar el compliment de calendaris, fites, superació de barreres i implicació dels actors involucrats. Consolidar i aportar iniciatives que permetin la presa de decisions operatives i estratègiques. Realitzar el reporting del servei. Donar suport a la realització / verificació d'estimacions de nous serveis dins del manteniment evolutiu. Gestionar adequadament la demanda del servei per tal d'assegurar l'adaptabilitat i la màxima qualitat.

-TÈCNIC ESPECIALISTA EN RESPOSTA A INCIDENTS DE SEGURETAT DE LA INFORMACIÓ amb les funcions de: Recopilació, classificació, etiquetat i registre de tota la informació associada a l'incident. Lideratge, anàlisi, i definició de la línia d'actuació per afrontar l'incident. Suport i assistència a comitè de crisi i reunions que es derivin de la gestió de l'incident. Participació en processos dins l'àmbit legal, cadena de custòdia d'evidències, defensa del cas, etc. Definició, seguiment i reporting de les accions in situ de contenció, mitigació i eradicació de l'incident. Participació en la gestió d'evidències, des de la seva obtenció, anàlisi i preservació. Redacció i/o suport en la generació de lliurables de seguiment, tècnics i executius. Propostes de millora, anàlisi i definició de processos de gestió, resolució de problemàtiques, metodologia, dins d'un procés de millora continu. Revisió, definició i creació de procediments i instruccions operatives. Relació amb tercers per la resolució d'un incident.

-AUDITOR DE SEGURETAT DE LA INFORMACIÓ amb les següents funcions: Suport a l'auditoria inicial a realitzar com a primera fase del servei de seguretat gestionada. Executar i coordinar els projectes d'auditoria tant de marc normatiu com de compliment legal (evolució i millora). Documentar i presentar els resultats de les auditories d'acord amb el sistema i metodologia de valoració i de reportat establert. Incorporar i mantenir la informació de les auditories a OneTrust.

-PROFESSIONAL CERTIFICAT EN SEGURETAT DE LA INFORMACIÓ per al: Suport en la definició, transformació, industrialització i formalització organitzativa de les diferents tasques del servei de seguretat gestionada. Suport en la definició, evolució, desplegament i seguiment d'un model de gestió de la seguretat de la informació per la UOC. Identificació d'oportunitats de millora i riscos en la gestió de seguretat en base a millors pràctiques. Execució de projectes

de seguretat de la informació en l'àmbit de la consultoria. Suport a tasques de realització de quadres de comandament.

La dedicació i les hores estan ben detallades fent un total de 140 hores anuals. Juntament amb la dedicació del coordinador del servei i de l'auditor (236 hores/any) fa que el dimensionament sigui correcte i suficient.

ERNST & YOUNG Global Limited fa una descripció molt detallada de cada perfil situant-lo dins una estructura organitzativa on podem observar el dimensionament global del servei a prestar.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

### 1.4.2. Viewnext

#### A: Solució proposada (fins a 3 punts)

No hi ha procediments associats a l'execució del servei i la proposta defineix únicament l'abast d'un anàlisi forense, no podent-se considerar com a tals.. El licitador tampoc proposa cap eina en la oferta.

La metodologia proposada es basa en múltiples normatives i guies com a marc de referència per a la recollida d'evidències, elaboració d'informes i tècniques forenses. Les metodologies citades en la oferta són: ISO-IEC 27037 per la recollida d'evidències, UNE-ISO 197001 per a l'elaboració d'informes, NIST-800-86 com a guia de tècniques forenses i la UNE 71506/2013 per a la documentació del informe pericial. Totes elles compleixen amb escreix les necessitats de la UOC.

El calendari no està definit. En tot cas l'anàlisi forense és un servei sota demanda i per tant no hi ha un calendari definit establert.

Les fases i les fites per a aquest servei no estan descrites. El licitador llista únicament una sèrie de punts en el que qualifica com els Punts que contindrà l'informe final i els punts que hauria de contenir un Informe Pericial. En tots dos casos no poden ser considerats com a fases del servei o fites.

La solució és incompleta ja que no abasta totes les tipologies de peticions que hauria de poder rebre el servei licitat. Especifica metodologies però no estableix fites ni especifica correctament les fases o els procediments, per tot això es considera que la descripció del servei és molt superficial.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

#### B: Recursos assignats (fins a 3 punts)

La proposta informa que l'equip proposat per fer l'anàlisi forense compartit amb el d'anàlisi de malware. Es defineixen un perfil amb dues categories professionals. Corresponent a:

- Perfil: Tècnic especialista en hacking ètic i pentesting:
  - Categoria 1: Auditor expert en seguretat
  - Categoria 2: Analista de seguretat

Les funcions de les categories del perfil, per aquest servei a prestar d'anàlisi de malware, són:

-AUDITOR EXPERT EN SEGURETAT: Responsable de l'execució de les tasques, Seguiment de les mateixes, Responsable del seguiment operatiu, Responsable de la supervisió i

coordinació, Realització dels informes , Preparació i presentació dels informes en les reunions, Anàlisi de millores i Garantir que les eines estan ben configurades i són les adequades.

-ANALISTA DE SEGURETAT: Elaborar i mantenir tota la documentació tècnica.

El dimensionament es el correcte. No cita les hores absolutes de dedicació, sinó que fa un percentatge del qual no indica la base a aplicar, per tant no permet conèixer el valor de les mateixes.

La descripció dels recursos és molt lleugera i poc concisa. Les funcions encara que detallades, no tenen pràcticament res a veure amb el servei i les tasques a realitzar. Així per exemple es parla d'un perfil "TÈCNICO ESPECIALISTA EN HACKIN ÈTICO I PENTESTING" que no següent el perfil adequat per aquest servei de ANÀLISI DE MALWARE.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.3. IThink UPC

### A: Solució proposada (fins a 3 punts)

Els procediments compleixen perfectament els objectius, i es fa una descripció en detall del mateixos, que son coherents amb la metodologia proposada: Etapa 1: Preservar i Adquirir Evidències, Etapa 2: Documentació, Investigació i Anàlisi i Etapa 3: Presentació de l'Informe. Les dues primeres etapes conformen la cadena de custòdia, la qual ha de demostrar que un element analitzat no ha pogut ser manipulat/alterat des de la seva recollida fins a la seva anàlisi.

El licitador proposa un ventall ampli d'eines d'anàlisi forense. Com ara: Cellebrite Touch, EnCase Forensics, Oxygen Forensic Suite, OSForensics, X-Ways Forensics per l'anàlisi forense en general. Però també per a l'adquisició d'Informació volàtil, d'Informació no volàtil, Especialitzades per a anàlisi forense mòbil, i altres tipus d'eines utilitzades en general o en el procés d'anàlisi forense.

El licitador exposa l'ús bàsicament de la metodologia UNE 71506. Però també de guies com RFC 3227, la NIST 800-86 i la ISO/IEC 27037:2012. Totes elles donen compliment al que es requereix en el plec tècnic. En aquest cas el calendari queda sota demanda del propi client.

Les fases per a aquest servei estan molt correctament descrites i al ser derivades d'una metodologia corresponen als procediments anteriors: Preservació (preservació de les dades volàtils i no volàtils sense alterar), Adquisició de les evidències (adquirir evidències preservant la cadena de custòdia i verificant la integritat en tot moment), Documentació (seguiment del procediment que s'ha efectuat fins ara), Anàlisi (anàlisi, investigació i exploració de totes les evidències recollides) i Presentació de l'Informe (tècnic, executiu i, si s'escau, proves judicials).

Les fites estan descrites en la proposta. Es valora molt positivament que s'inclogui la realització d'enquestes de satisfacció al client.

La solució aportada pel proveïdor està molt ben estructurada, és adequada a les necessitats exposades en el plec, les fites estan ben dimensionades i les eines són suficients i adequades. La solució aportada és correcta i coherent.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Es defineix la dedicació i les funcions a realitzar de forma correcte.

Els perfils assignats pel licitador per aquest servei són:

- Un especialista en infrasestructures de seguretat
- Un especialista en anàlisi forense
- Un professional certificat en seguretat
- Un auditor en seguretat i continuïtat de negoci
- Un coordinador del servei de seguretat
- Un gestor del servei

Les funcions assignades d'aquests perfils són: Vetllar per la provisió correcta del servei, Seguiment, Suport legal, Forensics de xarxes i comunicacions, Forensics de correus electrònics, Forensics de Windows, Forensics de Linux, Forensics de MacOs, Forensics d'Android i iOS, Altres forensics, Redactar informes executius, Emetre recomanacions sobre noves vulnerabilitats i amenaces, Documentar el procés de resposta a forensics.

El dimensionament de l'equip compleix el requerit al punt 4.2.1.3 del plec tècnic i inclús supera en un 15% al volum demanant

IThink UPC ha creat una matriu corresponent a perfils i funcions assignades amb un percentatge de dedicació a cada funció. El dimensionament és el correcte.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.4. (UTE) Opentrends + Cybernforce + Proficio

### A: Solució proposada (fins a 3 punts)

La proposta presentada per (UTE) Opentrends + Cybernforce + Proficio consta d'una descripció molt superficial del servei, es barregen conceptes amb serveis de monitorització, alertes i resposta a incidents.

S'expliquen les tasques i procediments per a una resposta a incidents, on hi podrien haver incidents d'anàlisi forense. El licitador no menciona eines específiques exceptuant l'ús general de la eina de Proficio. Les metodologies no estan descrites així com les fases per a aquest servei o les fites.

En aquest cas el calendari queda sota demanda de la UOC.

Per tot el que s´exposa, la solució aportada en la oferta és pràcticament inexistent per aquest servei d'anàlisi forense.

**1 punt**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta del licitador no s'identifiquen els recursos assignats, ni descriu la dedicació i funcions de cada un dels perfil, per tant, tampoc es pot avaluar el correcte dimensionament dels recursos.

- **0 punts**: La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

## 1.4.5. PricewaterhouseCoopers PwC

### A: Solució proposada (fins a 3 punts)

El licitador fa una proposta detallada i coherent de la solució. Es detallen els passos a seguir per la realització de les tasques del servei.

Els procediments compleixen els objectius del plec, i es fa una descripció dels mateixos amb més detall en les fases del servei. Encara que cita que l'anàlisi forense realitzat "no es referirà als aspectes o conseqüències legals dels mateixos", cosa que no està alineada amb el que es demanava en el plec a l'apartat 4.2.1.4.1.

El licitador explica que usarà eines que faciliten l'automatització, com ara Encase i d'altres eines Open Source però què no cita.

El licitador no proposa metodologies estàndards o pròpies

El calendari queda sota demanda de la pròpia UOC.

Les fases per a aquest servei estan correctament descrites i en resum són: Pas 1: Adquisició d'evidències digitals, Pas 2: Anàlisi tècnic de les evidències, Pas 3: Localització passiva de la informació, Pas 4: Anàlisi forense de les evidències i Pas 5: Elaboració d'informes.

No s'han trobat fites descrites en la proposta.

La solució aportada pel proveïdor està ben detallada. No obstant, la proposta no contempla metodologies, ni fites. Tot i que és coherent i l'ordre de les fases també ho és,no hi ha aplicada una metodologia ni es pot aplicar en totes les tipologies de peticions. Tanmateix hi ha algun aspecte relacionat amb els lliurables que podria no quedar cobert del plec com ara el Desenvolupament i realització d'informes pericials en cas d'un possible delicte o que s'hagi d'acreditar l'activitat ocorreguda davant d'un tribunal de justícia, el Desenvolupament d'informes adhoc pel Delegat de Protecció de Dades de la UOC i les agències estatals i autonòmiques de protecció de dades i les Certificacions informàtiques de fets, esdeveniments, estats, publicacions, etc. a l'estil fe notarial, però amb els mitjans informàtics forenses.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els recursos plantejats pel licitador no queden clarament assignats i es parla només d'un Panell d´ Experts i Suport amb les funcions de: Anàlisi (Activitats d'anàlisi forense) i Desenvolupament i millora de procés. Tots dos aspectes descrits de forma molt somera.

Les funcions, per tant, estan descrites d'una forma massa superficial.

En la oferta presentada per PricewaterhouseCoopers es parla d'un " Panell d´ Experts i Suport" que no permet identificar el recurs. El dimensionament no és el correcte.

**1 punt**: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.6. S2Grupo

### A: Solució proposada (fins a 3 punts)

El licitador proposa metodologies basades en la guía *Guide to Integrating Forensic Techniques into Incident Response Special Publication 800-86*. S'ajusten al que demana el plec.

No es defineixen a l'oferta els punts següents: procediments, eines o mitjans, calendari (tan sols s'indica que s'actuarà arrel d'un incident de seguretat), fases, ni fites.

La descripció està inclosa dins el servei de gestió d'incidents de seguretat d'una forma molt bàsica, ja que no s'inclouen procediments ni eines per exemple. Això invalida la possibilitat que la UOC pugui plantejar peticions incloses en la tipologia descrita al plec.

Això fa que la proposta no sigui del tot detallada, no donant compliment al que es requeria en els criteris de valoració. No obstant, s'aporten metodologies i una descripció de fases que es duran a terme en un anàlisi forense arrel d'un incident de seguretat.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta inclou una definició per nivells 2 i 3, però no es relacionen amb els diferents perfils ni les tasques a executar. Les funcions estan descrites d'una forma molt superficial. El dimensionament és el requerit en el plec.

Es defineix un rol de tècnic forense adient per a aquest servei, n' obstant, no s'atribueixen funcions.

Per tot el que s'ha exposat anteriorment, es considera que la proposta no compleix amb tots el punts que es valoraven en aquest apartat.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.

- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.7. S21Sec

### A: Solució proposada (fins a 3 punts)

La proposta no inclou un servei d'anàlisi forense pròpiament. Es fa constar en el punt de resposta a Incidents, però no hi ha descripció per a aquest servei.

L'oferta no defineix els punts següents: procediments, eines o mitjans, metodologies, calendari, fases, ni fites.

**0 punts**. La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### B: Recursos assignats (fins a 3 punts)

Els perfils definits en la proposta són els següents:

- Perfil: Enginyer/Nivell 3 i Auditor/Analista forense
- Funcions:
    - Revisió y resolució d'incidents de seguretat escalat pel nivell 2
    - Gestió avançada de dispositius de seguretat
    - Nivell màxim de col·laboració amb l'equip de serveis Avançats de Ciberseguretat
    - Coordinació de l'equip de resposta a incidents
    - Creació d'informes, plans d'actuació i millora.

El perfil que s´ha inclòs no té una descripció especifica. Les funcions que es detallen no corresponen amb el servei d'anàlisi forense. Està més centrat a resposta incidents. El dimensionament és el requerit en el plec

Volumetria: s'estimen 5 anàlisis a l'any. Dedicació de 96 hores / any.

S21Sec no descriu el perfil ni les funcions que es deriven d'aquest servei. Tan sols es fa un dimensionament genèric d´acord a les dades del plec.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.8. SAYTEL SERVICIOS INFORMÁTICOS

### A: Solució proposada (fins a 3 punts)

Els procediments estan correctament descrits amb les fases que es demanen. Les fases per a aquest servei estan extensament descrites de forma adient a les necessitats del servei. Les fases descrites a l'oferta són les següents: Fase de Comunicació, Fase d'adquisició de dades, Fase custodia i precintat, Fase d'anàlisi de dades, Fase de recopilació d'evidències i fets, Fase d'elaboració d'informes pericials (opcional), Fase de presentació de resultats.

Es descriuen les eines de les quals es composa el seu laboratori d'anàlisi forense, fem notar per exemple, eines de clonat forense en dispositius mòbils. Entre d'altres: Eines OSINT, Kit d'eines d'anàlisi forense Distribució Kali Linux: Binwalk, bulk-extractor, Capstone, chntpw, Cuckoo, dc3dd, ddrescue, DFF, diStorm3, Dumpzilla, extundelete, Foremost, Galleta, Guymager, iPhone Backup Analyzer, p0f, pdf-parser, pdfid, pdgmail, peepdf, RegRipper, Volatility, Xplico. També disposen de Memòries USB amb fitxers bootables, Eines de clonat Forense dispositius mòbils: Celebrity, Eines de clonat de disc dur: Tableu Forensic Duplicator, Lector de targetes, Càmera fotogràfica, Cables i adaptadors, Etiquetadora, Formularis d'adquisició.

El licitador no proposa cap metodologia ni es descriuen les fites per al servei. No es menciona calendari, ja que per a aquest servei seran peticions sota demanda.

La solució aportada pel proveïdor està ben estructurada, és adequada a les necessitats exposades en el plec. No obstant, no presenta fites, no està basada en cap metodologia que citin en la oferta. Les fases de la solució són coherents i les eines usades són correctes i adequades. L'ordre en que es realitzen les tasques és coherent.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils que incorpora la oferta són els següents:

- Tècnic especialista en resposta a incidents de seguretat de la informació, especialitat pèrit analista forense (90% dedicació sobre el total d'hores estimades):
    - Creació de peticions d'investigació, en el cas l'anàlisi forense derivi d'un servei de resposta a incidents.
    - Parametrització de les eines del laboratori per a la anàlisis.
    - Tasques d'adquisició de dades.

    - Tasques de custodia i precintat.
    - Anàlisi de les dades per l'obtenció d'evidències.
    - Documentació i evidencia trobades en l'anàlisi i informes pericials.
    - Documentació de proves i resultats obtinguts.
- Auditor en seguretat de la informació i continuïtat de negoci (10% dedicació sobre el total d'hores estimades):
    - Realització d'informes sota demanda per al DPO i la AEPD.

La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats i les seves funcions.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.4.9. T-Systems

### A: Solució proposada (fins a 3 punts)

La proposta inclou de forma esquemàtica les diferents fases del servei:

- Planning
- Acquisition
- examination
- interpretation
- reporting

Tanmateix, no es detallen a l'oferta els següents punts: procediments, eines o mitjans, metodologies, calendari ni fites.

La proposta còpia de forma literal el que s'especifica dins el PPT. No permet saber quina seria la proposta del licitador perquè no explica ni metodologies, ni descriu eines ni hi ha una explicació de les tasques o fases a realitzar. L´únic punt que inclou la proposta és la enumeració de forma esquemàtica de les fases del servei. Per tot el que s´ha exposat anteriorment, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest apartat.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta descriu 5 perfils dins d'aquest apartat, però no hi ha identificació clara amb el servei a prestar. Es barregen els perfils dels altres serveis sense poder discernir quina dedicació i funcions es duran a terme per a aquest servei d'anàlisi de malware. Les dades aportades en la proposta no permeten deduir el correcte dimensionament de la mateixa.

Per tot el que s´ha exposat anteriorment, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest apartat.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:

- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

# 1.5. Manteniment, revisió, administració i reporting de la infraestructura de seguretat de la UOC (fins a 6 punts)

## 1.5.1. ERNST & YOUNG Global Limited

### A: Solució proposada (fins a 3 punts)

El licitador ERNST & YOUNG Global Limited ha fet una proposta molt ben estructurada, que dóna resposta a tots els criteris de valoració i que afegeix alguna proposta de millora que pot servir perfectament als interessos de la UOC.

Els procediments en forma de activitats i tasques addicionals estan perfectament descrits i es pot considerar que satisfan completament els requeriments del plec de la UOC. Aquests procediments queden descrits gràficament correctament en fluxograma.

Les eines descrites són congruents amb les especificades al plec i en aquest cas no aplica l'ús d'eines específiques més enllà de les pròpies de connectivitat.

El licitador proposa una metodologia pròpia basada en NIST i els atacs més rellevants segons ISACA. Totes dues són adients pels requeriments del plec.

El calendari i les fites associades estan perfectament descrites i són coherents amb la proposta tècnica. Es valora positivament que el licitador comenci a per propostes de millora a partir de la 1a setmana.

Les fases del servei en forma d'activitats associades estan ben descrites i en alguns casos s'aporten activitats noves de millora a les inicials descrites al plec. Bàsicament són:

- Red Team: Avaluació de l'eficàcia de les activitats de protecció i prevenció davant de ciberatacs amb tests d'efectivitat continus.

-Revisió de casos d'ús de ciberatacs i creació de models/plantilles/documents per actuar davant els mateixos.

- Reforçar el valor de les activitats operatives de l'eina SIEM, com a eina principal del perímetre, i els seus processos.

Les fites descrites són molt correctes i pertinents a les tasques a realitzar. En resum són: Connexió EY Cybersecurity Operations Center, Accessos a eines de seguretat de la UOC, així com accessos per exemple al JIRA o SIEM, Auditoria de l'estat de les eines, així com els fluxes de treball i matrius d'escalat per grups, Pla anual de manteniment i millores de les eines, Processos i fluxes de treball, manteniment, operació i gestió de canvis, Accions / sessions de comunicació i formació dels processos a les parts interessades, Posada en marxa del servei de manera parcial, Posada en marxa servei de manera total, Evolució del SIEM – QRadar en termes d'integració de fonts, recepció d'esdeveniments, casos d'ús, regles de correlació, organització d'ofenses, etc, Evolució del ARBOR Pravail, TrendMicro TippingPoint 660N – Execució de les tasques d'evolució per aquesta eina i Firewalls Palo Alto i

Netscreen.

El licitador ha fet una bona descripció de les activitats a realitzar i les millores associades són molt interessants per la UOC, especialment l'enfocament del projecte basat en la creació de models i documents a partir de ciberatacs o el reforçament de l'activitat operativa del SIEM.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei, indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils estan molt ben definits, tan pel que fa a la seva descripció, activitats i perfil proposat. Aquests perfils es composen de:

> -COORDINADOR DEL SERVEI DE SEGURETAT amb les funcions de: Realitzar el seguiment del servei continuat i de les activitats que poden ser peticionades de manera discreta. Seguir i gestionar possibles desviacions de la planificació i pressupost. Coordinar el compliment de calendaris, fites, superació de barreres i implicació dels actors involucrats. Consolidar i aportar inciatives que permetin la presa de decisions operatives i estratègiques. Realitzar el reporting del servei. Donar suport a la realització / verificació d'estimacions de nous serveis dins del manteniment evolutiu. Gestionar adequadament la demanda del servei per tal d'assegurar l'adaptabilitat i la màxima qualitat.
>
> -TÈCNIC ESPECIALISTA EN GESTIÓ I ADMINISTRACIÓ DE SISTEMES SIEM amb les funcions de: Monitorització del correcte funcionament. Revisió de les ofenses que es detecten descartant falsos positius i generant tickets necessaris de treball. Revisió i manteniment de dashboards. Revisió i manteniment de casos d'ús i regles de correlació. Revisió i manteniment del correcte funcionament de les fonts integrades d'esdeveniments. Documentació i control de versions de la documentació associada: procediments, casos d'ús, protocols de resposta. Integració de processos existents o realització de nous i serveis adients. Integració de les solucions de ciberseguretat. Programació, modificacions de d'APIs i tasques d'operació i administració. Gestió de canvis, control de qualitat i de versions. Definició, implantació i millora de processos, fluxes de treball i autoritzacions.
>
> -AUDITOR DE SEGURETAT DE LA INFORMACIÓ amb les següents funcions: Suport a l'auditoria inicial a realitzar com a primera fase del servei de seguretat gestionada. Executar i coordinar els projectes d'auditoria tant de marc normatiu com de compliment legal (evolució i millora). Documentar i presentar els resultats de les auditories d'acord amb el sistema i metodologia de valoració i de reportat establert. Incorporar i mantenir la informació de les auditories a OneTrust.

- I un ENGINYER D'EINES DE SEGURETAT per a la: Creació de polítiques i controls de seguretat. Instal·lació, administració i manteniment d'eines de seguretat. Evolució de les solucions de seguretat de protecció, detecció i resposta. Monitorització del correcte funcionament. Generació d'alertes, regles de detecció i informes dels sistemes. Suport en la definició de nous projectes i definició de proves funcionals dels elements de seguretat. Documentació i control de versions dels desenvolupaments realitzats. Integració de processos existents o realització de nous i serveis adients. Integració de les solucions de ciberseguretat. Programació, modificacions de d'APIs i tasques d'operació i administració. Gestió de canvis, control de qualitat i de versions. Suport tècnic i assessorament projectes, infraestructura i solucions. Definició, implantació i millora de processos, fluxes de treball i autoritzacions. Realització de pla d'actuació trimestral amb iniciatives d'evolució i transformació.

La dedicació i les hores estan ben detallades fent un total de 880 hores anuals. Juntament amb la dedicació del coordinador del servei i de l'auditor (236 hores/any9  fa que el dimensionament sigui correcte i suficient.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.2. Viewnext

### A: Solució proposada (fins a 3 punts)

El licitador Viewnext fa una proposta molt parcial de les activitats i requeriments que la UOC especifica en el seu plec i la centra bàsicament en el suport al manteniment de les diferents plataforma en lloc de la gestió de les mateixes. No obstant es valora positivament que el licitador ofereixi actuacions presencials quan el servei ho requereixi.

No s'han pogut trobar en sentit estricte els procediments o les activitats relacionades amb la prestació del servei, i les que es citen són a un nivell massa genèric.

Les eines descrites i plataformes a les que donar servei són les especificades en el plec.

No s'ha pogut trobar cap metodologia associada al servei. Igualment no s'ha pogut trobar, tampoc, cap calendari ni les fites associades. Les fases del servei no estan descrites com tal i únicament es citen alguns acords més propis de un ANS. No hi ha fites descrites pel servei en qüestió.

El licitador ha fet una descripció molt parcial i incompleta de les activitats, fases i procediments a realitzar. És valorable que el licitador s'ofereixi a desplaçar-se a les dependències de la UOC en cas que fos necessari o que el servei ho requerís.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils estan molt poc definits, i no s'acaba d'entendre massa bé la assimilació que es fa per part del licitador entre la categoria professional descrita i el perfil assignat. Tanmateix els perfils que es descriuen no s'acaben d'entendre del tot bé, així: "*Técnico Analista de Infraestructura de Seguridad; analizarán y desarrollarán la técnica de sistemas necesaria para implantar la plataforma Infraestructura de Seguridad y supervisará el correcto funcionamiento de la plataforma*.". Què no correspon amb cap perfil i no cobreix les necessitats de la UOC, ja que és mes aviat un perfil d'Administrador de Sistemes.

Les funcions estan poc detallades per cadascun dels perfils i la dedicació en hores no està descrita. Això fa que el dimensionament no quedi definit correctament.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.3. IThink UPC

### A: Solució proposada (fins a 3 punts)

iThink UPC ha fet una molt bona proposta referent a l'ús de metodologies de gestió de serveis i de gestió de projectes associades al servei licitat. Tanmateix fa una proposta menys detallada sobre les activitats a realitzar en el si del servei i remet el calendari a fora de l'àmbit del límit de pàgines disponibles per la descripció d'aquest servei.

Els procediments estan molt ben detallats de forma general per tots els dispositius i activitats del servei. El model operatiu i els procediments associat estan molt ben descrits i aporten valor a la proposta. En resum el licitador estableix dos grups de procediments que després desenvolupa en la oferta: Procediments genèrics de resposta a esdeveniments, en funció de la infraestructura i la criticitat i Procediments específics de resposta a esdeveniments complementaris als anteriors.

Les eines descrites són congruents, detallades i útils respecte al que s'especifica en el plec. A més a més aporten aspectes de millora com ara les automatitzacions de tasques. Una llista d'aquestes eines és: KeePass, Puppet per la gestió de sistemes per polítiques, Rundeck per a l'automatització i programació de tasques i Emailtomatic programari propietari del licitador per al processat intel·ligent de mails.

Les metodologies descrites són molt correctes i es corresponen a les necessitats de la UOC. Aquestes són: metodologies de gestió de serveis TIC (ITIL, ISO 20000 i ISO 27001) i metodologies de gestió de projectes (PMBOK).

El calendari, donat que en certa manera és subsidiari de l'adquisició de coneixement per part del licitador, es remet al Punt 4 del plec de les Fases de Prestació del Servei.

Les fases del servei s'expliquen en forma d'activitats associades com ara: Detecció i validació de l'alerta o esdeveniment, Identificació del procediment de resposta que tingui associat, Execució del procediment (o més d'un si fos el cas), Registre de l'alerta i el seu tractament mitjançant l'obertura d'un tiquet a l'eina Jira, Classificació i categorització, Notificació a l'interlocutor associat, si s'escau, Associació de les infraestructures afectades, Assignació del tiquet a l'interlocutor del servei definit, si s'escau i Tancament del tiquet després de la recuperació de l'alerta.

Les fites són correctes i s'ajusten als criteris de valoració. Es valora positivament que s'inclogui la realització d'enquestes mensuals de satisfacció al client.

El licitador ha fet una descripció correcta del servei. Aporta una sèrie de criteris de valor com ara algunes opcions de millora i el model operatiu i procediments associats. Tanmateix es valora molt positivament les enquestes com a fita de valor afegit o les eines d'automatització.

**3 punts:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció detallada de la proposta organitzativa per assolir la prestació del servei,

indicant el calendari, les fases i les fites que es duran a terme en l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Es defineix la dedicació i les funcions a realitzar de forma correcte.

Els perfils assignats pel licitador per aquest servei són:

- Un professional certificat en seguretat
- Un especialista en gestió i administració de sistemes SIEM
- Un professional certificat en seguretat
- Un coordinador del servei de seguretat
- Un gestor del servei

S'aporta el detall de dedicació de cada perfil: Vetllar per la provisió correcta del servei, Seguiment, Gestió de l'Arbor, Gestió del Trendmicro, Gestió del FWs (Palo Alto, Fortinet), Gestió del Qradar, Atenció de primer nivell i alarmes, Redactar informes executius, Emetre recomanacions sobre noves vulnerabilitats i amenaces, Documentar el procés de gestió d'infraestructures.

El dimensionament de l'equip compleix el requerit al punt 4.2.1.3 del plec tècnic i inclús supera en un 15% al volum demanant de 682 hores.

IThink UPC ha creat una matriu corresponent a perfils i funcions assignades amb un percentatge de dedicació a cada funció. El dimensionament és el correcte.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts**: La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.4. (UTE) Opentrends + Cybernforce + Proficio

### A: Solució proposada (fins a 3 punts)

El licitador Opentrends + Cybernforce + Proficio fa una oferta que no s´ajusta al que sol·licita en el plec de la UOC. El licitador fa referència a l'ús d'una eina anomenada Proficio MMS que pot gestionar remotament equips de seguretat, però en cap moment especifica que els equips citats en el plec siguin compatibles amb aquesta solució.

No s'han trobat procediments associats en la oferta.

La única eina de la que és parla és Proficio MMS, però amb la descripció que facilita el licitador no es pot determinar si és coherent amb les activitats del plec. Falta més informació.

No hi ha metodologies descrites. No s'ha pogut trobar cap calendari associat. Tampoc s'han trobat fases del servei. Ni tampoc hi ha fites associades al calendari.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

La proposta del licitador no s'identifiquen els recursos assignats, ni descriu la dedicació i funcions de cada un dels perfil, per tant, tampoc es pot avaluar el correcte dimensionament dels recursos.

- **0 punts**: La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

## 1.5.5. PricewaterhouseCoopers PwC

### A: Solució proposada (fins a 3 punts)

La proposta inclou una transcripció literal del plec tècnic. A tall d'exemple el que es cita en la descripció de la primera activitat: "*La tercera y última capa de nuestra aproximación consiste en la gestión funcional del propio servicio de Operación y Mantenimiento de herramientas de Seguridad IT tal y como figure en el contrato*".

Tanmateix el calendari proposat fa un pla de revisió i reporting únicament una vegada a l'any i a l'inici del projecte, quan hauria de ser un procés més iteratiu i continuat. La proposta de gestió de processos basada en ITIL és bona i s´ajusta a les necessitats del servei.

Les activitats i procediment descrits per cadascuna de les solucions de seguretat recullen només de forma parcial el conjunt d'activitats del plec. Igualment en la descripció genèrica dels procediments hi ha alguna incongruència, com quan es parla del model de gestió d'una Oficina de Seguretat. Quan això no és l'objecte del servei.

No s'han trobat ni eines ni mitjans associats a l'execució del servei.

El licitador explica que les metodologies que utilitzarà estan basades en ITIL, ajustant-se a les necessitats del servei.

la proposta inclou un calendari que està associat a una sèrie de recursos els quals donen compliment als requeriments del servei.

Per altra banda, la proposta no inclou les fases del servei. Tanmateix les activitats a realitzar tampoc estan descrites en detall i es lliguen a la evolució del projecte sense més.

No s'ha pogut trobar fites associades al servei o al calendari.

El licitador ha fet una proposta correcta però amb una certa superficialitat especialment en la descripció dels procediments i les fases del servei.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant, per cada tasca:
  - El procediment que seguirà el proveïdor per gestionar-la
  - Els mitjans que s´utilitzaran
  - Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec

- I, una descripció de la proposta organitzativa on no s'ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

## B: Recursos assignats (fins a 3 punts)

Els perfils i funcions que incorpora la proposta són:

> - Perfil d'ESPECIALISTA EN GESTIÓ I ADMINISTRACIÓ DE SISTEMES SIEM (I D'ALTRES SOLUCIONS DE SEGURETAT). Amb les següents funcions: Desenvolupar el pla de manteniment, revisió i reporting, així com Desenvolupar els manuals pertinents associats al servei i el Manteniment, revisió i reporting continuat.
>
> - Perfil d'AUDITOR EN SEGURETAT DE LA INFORMACIÓ I CONTINUÏTAT DE NEGOCI. Amb les següents funcions: Anàlisi documental existent, Documentació de vendors, Manuals Operatius i Manteniments existents.

Les funcions previstes que exposa el licitador no tenen massa a veure amb l'objecte del servei i en qualsevol cas es fa d'una manera molt genèrica. Les funcions de cadascun dels perfils no estan del tot relacionades amb el demanat en el punt 4.2.1.5.1 del plec. Tot i això, la proposta si que descriu correctament la dedicació de cadascun dels perfils.

Pel que s´ha exposat, el dimensionament no s´ajusta a les necessitats del servei.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt**: La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou:
    - Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.6. S2Grupo

### A: Solució proposada (fins a 3 punts)

La proposta no descriu cap dels criteris de valoració descrits en el plec UOC. La proposta parla de que el servei que s'oferta és una guia personalitzada per a preservar la correcta operativitat de cada dispositiu quan en realitat el que es demanava en el plec és una explotació total del dispositiu, les seves dades i la operativa del mateix.

No es defineixen a l'oferta els següents punts: procediments, mitjans o eines, metodologies, calendari, fases del servei, ni fites.

**0 punts:** Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### B: Recursos assignats (fins a 3 punts)

Dels perfils presents en la oferta, només es pot identificar el relacionat amb el SIEM. La proposta no inclou les funcions ni la dedicació específica del perfil que s'ha identificat. Tenint en compte això, la proposta no inclou el dimensionament.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.

La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.7. S21Sec

### A: Solució proposada (fins a 3 punts)

S21Sec fa una interpretació dels requeriments del plec que no s'ajusta a les activitats demanades per la UOC. Així el licitador explica que el servei inclou “totes les activitats incloses en el suport preventiu dels equips tals com les actualitzacions”. Aquest fet no està en cap moment citat com a activitat i sí, en canvi, s'especifica que la operació dels dispositius correrà a càrrec exclusivament del servei d'operacions de la UOC.

L’oferta no defineix els punts següents: procediments, eines o mitjans, metodologies, calendari, fases, ni fites.

**0 punts**. La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### B: Recursos assignats (fins a 3 punts)

Els perfils que incorpora la oferta són:

- Perfil: Enginyer
- Funcions:
    - Implantació de dispositius
    - Execució i generació de documentació
    - Realització de consultories
    - Entre d’altres…

Els perfils, encara que presents en la oferta, estan definits de manera molt genèrica. Es parla només d´enginyers. Les funcions estan llistades d'una manera molt genèrica i no es poden associar directament a un perfil en concret. La dedicació està descrita en hores però no assignada a un o uns perfils en concret. Amb les dades proporcionades, no és possible conèixer si el dimensionament és el correcte.

Per tot el que s’ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.8. SAYTEL SERVICIOS INFORMÁTICOS

### A: Solució proposada (fins a 3 punts)

SAYTEL SERVICIOS INFORMÁTICOS ha fet una proposta correcta que cobreix totes les activitats especificades en el plec. Tanmateix ofereix una sèrie d'activitats a realitzar per a totes les plataformes i solucions que aporta valor a la oferta del licitador, establint els procediments a seguir.

Les fases del servei proposades són correctes i satisfactòries per les necessitats i requeriments del servei. Les fases descrites són: Fase de Comunicació, Fase d'adquisició de dades, Fase proposta de canvi de configuració al grup operatiu, Fase de monitorització d'indicadors i dashboards, Realització d'informes i documentació.

No s'han descrit en aquesta oferta els següents punts: eines o mitjans, metodologies, calendari ni les fites.

El licitador ha fet una descripció correcta del servei. Aportant una sèrie de criteris de alt valor com ara el manteniment de la documentació operativa, l'anàlisi de tendències de capacitat i d'altres. Malgrat tot no es poden valorar les fites, eines, metodologies i calendari ja que no s'ha pogut trobar en la oferta.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils descrits en l'oferta són els següents:

- Equip Tècnics especialistes en gestió plataformes de seguretat perimetral:
    - Tasques realitzades sobre el Sistema ARBOR:
        - Revisió diària de la consola de gestió.
        - Revisió diària de les gràfiques de bloquejos.
        - Revisió setmanal dels llindars d'ample de banda.
        - Revisió dels grups de protecció - Inbound Protection Groups.
        - Revisió i actualització mensual dels Profile Capture.
        - Revisió dels informes del servidor.
        - Captura de paquets en cas de conflicte o investigació.
        - Generació d'informes
    - Tasques realitzades sobre el Sistema TrendMicro TippingPoint:
        - Revisió diària dels esdeveniments més destacats per nivell de severitat.
        - Revisió diàriament els esdeveniments generats pel dispositiu cercant patrons o qualsevol altre tipus d'indici que pugui significar l'existència d'un risc o vulnerabilitat.

        - Elaboració de propostes de canvi o millora en les polítiques del dispositiu, per tipus de tràfic.
        - Revisió dels Responders i manteniment dels mateixos.
        - Participació en les reunions del grup de sistemes.
        - Elaboració d'informes.
    - Tasques realitzades sobre el Sistemes Tallafocs:
        - Definició un procediment organitzatiu de flux d'aprovacions de canvis en les polítiques de firewalling.
        - Confecció d'un mapa senzill de regles o catàleg fàcilment consultable.
        - Anàlisi i proposta de millora a nivell funcional de les polítiques dels diferents dispositius.
        - Realització d'informes d'activitat maliciosa.
        - Anàlisi i captura de paquets.
        - Resposta a consultes sobre la configuració d'algunes de les regles.
- Tècnic especialista en gestió i administració de sistemes SIEM:
    - Revisió diària de la consola del dispositiu cercant mal funcionaments, avisos i errors. En cas positiu, generarà les corresponents ordres de treball al grup operatiu o proveïdor corresponent.
    - Revisió diària de les ofenses que detecta el dispositiu. Generació dels tiquets de treball necessaris perquè dites ofenses siguin resoltes pel grup operatiu UOC corresponent.
    - Revisió i manteniment dels dashboards de QRadar.
    - Revisió i manteniment de les fonts de log.
    - Manteniment dels diferents sub-sistemes i serveis de QRadar: Network Hierarchy, Index Management, Asset Profiler, Custom Asset Properties, DSM Editor, Log Sources, Custom Event Properties, Event Retention, User Behavoir.
    - Gestió dels informes que es poden generar des del mateix dispositiu QRadar.
    - Realització de tasques de manteniment pertinents sobre el sistema de pre-processat de logs.

Les funcions i la assignació d'aquestes al perfil, així com el seu dimensionament estan ben definits i s´ajusten als requeriments del servei.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma detallada als criteris que es valoren en aquest punt.

**3 punts:** La proposta presenta un dimensionament coherent sobre els requeriments, així com la idoneïtat dels perfils assignats, on s´inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

## 1.5.9. T-Systems

### A: Solució proposada (fins a 3 punts)

El licitador T-Systems fa una descripció de la seva proposta de servei on es recolza bàsicament en que per cada solució afirma que es faran les tasques que la UOC ha definit en el seu plec, sense donar cap més explicació ni dir com les farà. No s'ha pogut valorar cap més criteri donat que la resta són inexistents per a aquest servei concret.

No hi ha cap procediment escrit i l'únic que se cita és que les activitats a realitzar són les descrites en el plec. És valorable que es digui que es farà un procediment de canvis de política de seguretat.

No queden definits en l'oferta els següents punts: eines o mitjans, metodologies, calendari, fases ni fites.

El licitador ha fet una descripció molt superficial per la prestació d'aquest servei i sempre remetent-se a que les activitats són les citades en el plec, però ometent explicar com ho farà.

Per tot el que s´ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta inclou:

- Una descripció detallada de la proposta tècnica, tot especificant per cada tasca:
- El procediment que seguirà el proveïdor per gestionar-la
- Els mitjans que s´utilitzaran
- Metodologies proposades

que permeti assolir els requeriments funcionals i tecnològics indicats en el plec.

- I, una descripció de la proposta organitzativa, on no s´ha inclòs algun dels següents elements (i) el calendari, (ii) les fases, (iii) fites que es duran a terme per l'àmbit valorat.

### B: Recursos assignats (fins a 3 punts)

Els perfils estan definits encara que exceptuant el coordinador, la resta no tenen massa relació amb aquest servei en concret. Les funcions encara que citades no hi tenen massa a veure amb el servei en qüestió i no permet afirmar que siguin les més indicades pel servei. La dedicació està expressada en percentatge, però no s'indica sobre quin valor s'ha d'aplicar aquest tant per cent.

Els perfils que inclou la proposta són:

- Customer Security Manager (CuSM) amb un rol de coordinador de servei i una dedicació del 20%. Les seves funcions són: Coordinació, comunicació, seguiment, informes, reunions.
- Analista N2 amb un rol de tècnic especialista Hacking i una dedicació del 30%. Les seves funcions són: anàlisi de vulnerabilitats, pentesting, documentació, operació.
- Auditor N1 amb un rol d´auditor de seguretat i una dedicació del 10%. Les seves funcions són: auditories i informes.
- Analista N1 amb un rol de professional certificat i una dedicació del 50%. Les seves funcions són: anàlisi de riscos, informes, seguiment SGSI.
- Analista N3 amb un rol de tècnic especialista en resposta i una dedicació del 10%. Les seves funcions són: anàlisi forense, malware, resposta a incidents.

El dimensionament és correcte, no obstant, els perfils i les funcions descrites en aquest apartat no són adequades per a aquest servei.

Per tot el que s'ha exposat, es considera que la proposta dona compliment de forma parcial als criteris que es valoren en aquest punt.

**1 punt:** La proposta presenta un dimensionament coherent sobre els requeriments, però la idoneïtat dels recursos assignats no queda justificada. La proposta inclou:

- Identificació dels recursos assignats
- Dedicació i funcions de cada un dels perfils proposats d´acord a les tasques a executar.
- La proposta no inclou: Idoneïtat en el dimensionament dels recursos assignats a cada tasca definida.

La puntuació total obtinguda al segon apartat, anomenat **PROPOSTA DE PRESTACIÓ DEL SERVEI** és la següent:

| **Taula de puntuació** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Puntuació màxima** | **30 punts** | **Ernst&Young** | **Viewnext** | **iThink UPC** | **UTE Opentrends Cybernforce Proficio** | **UTE PwC** | **S2 Grupo** | **S21Sec** | **Saytel** | **T-Systems** |
| 1. Proposta de prestació del servei | **30** | | | | | | | | | |
| 1.1. Detecció, anàlisi i gestió de vulnerabilitats | **6** | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 3 | 1 | 1 | 3 | 1 |
| B. Recursos assignats | 3 | 3 | 3 | 3 | 0 | 3 | 1 | 1 | 3 | 1 |
| 1.2. Gestió i resposta a incidents de seguretat de la informació CSIRT | **6** | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 3 | 1 | 1 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 3 | 1 | 1 | 3 | 1 |
| 1.3. Anàlisi de malware | **6** | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 1 | 1 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| 1.4. Anàlisi forense | **6** | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 1 | 0 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| 1.5. Manteniment, revisió, administració i reporting de la infraestructura de seguretat de la UOC | **6** | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 0 | 0 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| | | 30 | 12 | 30 | 5 | 18 | 9 | 8 | 22 | 10 |

# 2. Gestió i governança del servei (fins a 5 punts)

## 2.1. Model de relació (fins a 1 punt)

### 2.1.1 ERNST & YOUNG Global Limited

La proposta d'ERNS&YOUNG descriu els perfils amb els que es tindrà interlocució a nivell estratègic, tàctic i operatiu, en concret, s'inclou el perfil del perfil de responsable/coordinador de servei detallant les funcions principals, entre altres, realitzar el seguiment del servei continuat relatiu al servei, seguir i gestionar possibles desviacions pel que fa a planificació i pressupost i realitzar el reporting del servei.

La proposta incorpora addicionalment la figura d'un sènior mànager amb funcions d'assegurar la qualitat i reforça al responsable del servei del proveïdor per assegurar l'acompliment dels ANS del servei i la millora contínua, per tant, aquest element garanteix la monitorització adequada del servei.

En quant a eines de comunicació per garantir l'èxit en el model de relació proposen entre altres, els informes de servei, el quadre de comandament online, i el JIRA de la Suite Atlassiant per la relació amb els equips tècnics.

També es detallen els tres comitès requerits en el punt 5.1 Model organitzatiu de l'equip de treball, estratègic, tàctic i operatiu, les seves funcions, s'informa de la periodicitat, el comitè estratègic trimestral i sota demanda, el nivell tàctic mensual i sota demanda i el nivell operatiu setmanal i els entregables que són els informes del servei, indicant la data de compromís a entregar la documentació, prèvia als Comitès i el detall del contingut dels entregables. Això permetrà un anàlisi previ per part dels assistents als comitès i, per tant, una presa de decisió àgil i argumentada. Es valora molt positivament que, en els entregables de cada comitè, no només s'analitzi el què ha passat durant el període, sinó que en cada un d'ells hi hagi propostes de millora, plans d'actuacions o detecció de futures necessitats, aquesta aportació assegura la millora contínua del servei.

Per tot l'exposat anteriorment, es considera que la proposta del proveïdor dona compliment de forma detallada a tots els punts que es valoren en aquest apartat.

**1 punt**: Si la proposta inclou:

Una descripció detallada del model de relació, on s´inclou:
- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció detallada dels comitès proposats, on s´inclouen:
- Les funcions de cadascun d´ells
- Les figures implicades
- La seva periodicitat
- Entregables a lliurar per part del proveïdor adjudicatari així com el seu contingut.

### 2.1.2 Viewnext

La proposta informa de la incorporació de la figura del coordinador del servei i de les seves funcions, principalment la d'assumir la responsabilitat de la gestió i el seguiment de les tasques del servei, i també d'un auditor expert en seguretat fent la funció de responsable del seguiment operatiu del servei.

També proposa una estructura de model de govern a tres nivells: estratègic, tàctic i operatiu, tal com s'especifica en el Plec de prescripcions tècniques, i descriu les funcions el primer assegurar l'estratègia i objectius, el tàctic seguiment de les activitats i l'operatiu revisió de l'estat dels serveis i activitats i la periodicitats dels comitès vinculats als tres nivells, semestral, mensual pels dos primers nivells. Tot i això, la proposta no especifica la periodicitat del nivell operatiu.

Per altra banda, la proposta no especifica els lliurables de cap d'ells ni cap altra eina de comunicació

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

0,5 punts: Si la proposta inclou:

Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.3 IThink UPC

La proposta detalla de manera exhaustiva dos perfils i les funcions per gestionar el servei: coordinador de servei i gestor de servei. Les funcions estan clarament identificades i diferenciades amb la característica que els dos es complementen donat que un té la funció principal de garantir l'acompliment del contracte i aspectes estratègics i, el segon, té la responsabilitat de garantir l'operativa diària. Els dos perfils participen en els comitès configurats al model de relació. Per tant, la proposta assegura la gestió del servei amb aquests dos perfils.

En quant als comitès requerits, estratègic, tàctic i operatiu, estan identificades les funcions, periodicitat correctament segons els requeriments, però en la descripció dels lliurables de cada comitè, s'indica que els lliurables del comitè tàctic i operatiu són els mateixos que el Comitè estratègic, considerem que aquests elements no han de ser els mateixos donat que un comitè té unes funcions de seguiment del contracte i del servei, i els altres tenen funcions d'analitzar vulnerabilitats o tasques o temes més operatius i del dia a dia. Per aquest motiu, si bé el model de relació és compleix el demanat en el plec tècnic, la proposta d 'entregables no s'adequa a les necessitats del servei.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts**: Si la proposta inclou:
Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions

- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.4 (UTE) Opentrends + Cybernforce + Proficio

En quant al model de relació, la proposta detalla tres rols : Director de Servei, Responsable de Servei i Team Manager. El primer rol pren les decisions sobre l'organització de la prestació del servei, el segon controla el compliment del contracte i la càrrega de treball i el darrer perfil, Team Manager, és el responsable de l'operativa i de complir els ANS, entre altres.

El detall dels Comitès de Govern que s´indica en la proposta,, no compleix el requerit en el plec de prescripcions tècniques, apartat 5, on es demana tres nivells d'interlocució : estratègic, tàctic i operatiu. Els nivells d'interlocució proposats són el nivell estratègic i nivell tàctic on sí existeix interlocució directa entre el responsable de servei del proveïdor i els responsables del servei de la UOC, en canvi, la proposta explica que el nivell operatiu l'aïllen i no ofereixen la possibilitat d'interlocució directe amb el responsable de servei de la UOC, de manera que la seva activitat només es pot seguir i avaluar per un conjunt d'informes.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts**: Si la proposta inclou:

Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.5 PricewaterhouseCoopers PwC

En la proposta s'indica la incorporació del rol requerit del responsable/coordinador del servei per part del proveïdor però no es detalla quines són les seves funcions. S'identifiquen quins són els informes pels 3 comitès requerits de nivell Estratègic, tàctic i operatius, però el contingut detallat només indica informació a nivell de seguiment dels indicadors i situació actual però no incorporen als informes plans de millora o futures accions.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat. .

**0,5 punts**: Si la proposta inclou:
Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions

- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.6 S2Grupo

La proposta informa de la incorporació del rols de Coordinador de Servei i de Responsable de servei però no detalla quines són les seves funcions. Per altra banda, es detallen les funcions dels tres comitès existents en el model de relació (estratègic, tàctic i operatiu) , tal com es requereix en el plec tècnic i informa els lliurables de cada comitè, tanmateix, no es detalla contingut de cada d'un d'ells.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts**: Si la proposta inclou:

Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.7 S21Sec

La proposta identifica la figura d'un Service Manager i les seves funcions, rol equiparable al de coordinador de servei que es requereix el plec tècnic. En quant al model de relació, proposa tres nivells (de Direcció, de Coordinació i Operatiu) que en les funcions especificades es poden equiparar als tres nivell demanats al plec tècnic (estratègic, tàctic i operatiu), ara bé, no detalla dels diferents Comitès ni la periodicitat, ni els entregables a lliurar.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** Si la proposta inclou:
Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.8 SAYTEL SERVICIOS INFORMÁTICOS

La proposta de SAYTEL SERVICIOS INFORMÁTICOS incorpora els rols de Coordinador de Servei i Coordinador del CSIRT però no detalla quines són les funcions de cada rol, tanmateix, sí informa de la seva participació en els diferents comitès. També la proposta detalla les funcions dels tres comitès existents en el model de relació, tal com es requereix en el plec tècnic, i informa dels lliurables i dels continguts en el cas del Comitè operatiu, però no en el cas dels Comitè Estratègic i del Tàctic.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts**: Si la proposta inclou:
Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

### 2.1.9 T-Systems

La proposta informa dels perfils que intervenen en l'execució del servei: Responsable del servei, Coordinador de servei i l'equip de seguretat. Tant en el cas de Responsable del servei com en el de Coordinador del servei no s'especifica quines són les funcions de cadascú tal com es demana en el punt.

Per altra banda, es detalla quins són els tres comitès que es composaran per la governança del servei, quins són els perfils que hi assisteixen, la periodicitat i les funcions del Comitè, tal com es requereix en el punt 5.1 Model organitzatiu de l'equip de treball del Plec de prescripcions tècniques, però, en el cas de Comitè expert en seguretat no es detallen els entregables.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts**: Si la proposta inclou:
Una descripció detallada del model de relació, on s´inclou:

- La figura de coordinació del servei i les seves funcions
- Descripció de les eines de comunicació que el proveïdor adjudicatari utilitzarà per tal de garantir l´èxit en el model de relació associat al servei.

I, una descripció dels comitès proposats, on no s´explica algun dels següents punts (i) les funcions de cadascun d´ells, (ii) les figures implicades, (iii) la seva periodicitat, (iv) els entregables a lliurar amb el seu contingut per part del proveïdor adjudicatari.

## 2.2. Metodologia, mecanismes de control i seguiment del servei (fins a 3 punts)

### 2.2.1 ERNST & YOUNG Global Limited

La proposta d'ERNS&YOUNG descriu amb detall la metodologia que ha d'assegurar la qualitat del servei indicant la periodicitat i la definint clarament les responsabilitats. En concret, detalla que la metodologia es basa en un procés proactiu, col·laboratiu, integrat en el cicle de vida del servei, recurrent (basat en el cicle de'Deming' o Pla-Do-Check-Act) i en temps real.

Com a elements de control i seguiment de la qualitat, es destaca la incorporació del rol de quality manager amb la funció de garantir els nivells de servei que actuarà fent auditories i revisions de la qualitat. També, proposen realitzar informes del resultat del seguiment de la qualitat del servei que s'entregaran previ als comitès de seguiment. El detall del continguts de l'informe de seguiment de la qualitat en la proposta, que conté entre altres el resum global de l'evolució dels SLA, els indicadors de qualitat i el resultat de les enquestes de satisfacció, ens asseguren la informació que es necessita per avaluar la prestació del servei i corregir o efectuar millores en cas necessari.

La Gestió de la qualitat que explica la proposta conté els processos de Pla de qualitat, assegurament de la qualitat i controls de la qualitat. Per cada procés es detallen les activitats, la periodicitat i la responsabilitat. En concret, el procés d'assegurament de la qualitat detalla que és el coordinador del servei qui serà el responsable i en el procés del Controls de qualitat es faran revisions i auditories de qualitat i estaran liderades pel quality manager.

També, la proposta especifica el procés de millora contínua, posant focus en els àmbits de seguiment dels nivells de servei, revisió dels entregables, gestió de l'equip, gestió de les incidències del servei, gestió de riscos, gestió de les expectatives i gestió del coneixement, entre altres, que ha de permetre millorar el servei de manera eficient i continuada. En concret, la gestió de riscos que detalla la proposta, es configura com un procés continu on es realitzen 6 activitats entre les que hi ha la identificació de les causes i de les conseqüències, l'avaluació de l'impacte i de la probabilitat i la definició del pla d'acció. Aquesta procés de gestió de riscos continu assegura la detecció temprana i correcció o mitigació dels riscos del servei.

Per tot l'exposat anteriorment, es considera que la proposta del proveïdor dona compliment de forma detallada a tots els punts que es valoren en aquest apartat.

**3 punts:** Si la proposta inclou:

- Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.
- I, una descripció detallada dels mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció i gestió de riscos, etc.)

### 2.2.2 Viewnext

La proposta de Viewnext informa la metodologia, model de control, del servei per garantir l'execució

que basant-se en la gestió dels indicadors del servei però no detalla els elements o mecanismes que han d'assegurar que es compleixin els indicadors, s'especifica que en els Comitès trimestrals es farà seguiment dels mateixos per trobar mesures correctores, fet que considerem insuficient per l'assegurament de la qualitat del servei. Per altra banda, no detalla el procés d'assegurament de la qualitat ni de control de qualitat.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.3 IThink UPC

La proposta d'IThink UPC informa que la metodologia que seguirà per garantir el compliment del servei es basa en ITIL i PMBOK, tanmateix no explica quins són els processos de gestió de la qualitat que s'implantaran, ni les activitats ni la periodicitat. La proposta explica alguns mecanismes per mesurar la qualitat, com les enquestes de satisfacció als usuaris, però no detalla el procés d'assegurament de la qualitat ni de control de qualitat.

En quant a la gestió de riscos, la proposta informa d'un Pla de Gestió de riscos però el detall es troba fora del rang de pàgines requerides a la proposta i no es pot avaluar.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.4 (UTE) Opentrends + Cybernforce + Proficio

La proposta de la UTE Opentrends + Cybernforce + Proficio, especifica que per assegurar la qualitat del servei es revisaran els estàndards de qualitat i seguretat en projectes de ciberseguretat portats a terme a l'organització, però no especifiquen quins són els estàndards ni l'objecte de l'assegurament de la qualitat que anomenen en el servei, sinó uns projectes que no són objecte de la contractació.

Per altra banda, expliquen la incorporació d'un administrador de projectes i un gerent de projectes per realitzar un seguiment de les tasques, la ruta crítica i la programació, quan l'objecte del present servei

a contractar no està contextualitzat en projectes sinó en servei, per tant, aquest model no correspon a la metodologia i els mecanismes de control i seguiment per assegurar la qualitat d'un servei.

L'únic mecanisme que aplica al servei requerit en el plec tècnic per l'assegurament de la qualitat del servei és el seguiment de la qualitat del suport 24x7.

El licitador UTE Opentrends + Cybernforce + Proficio, tal com es detalla anteriorment ,no ha descrit la metodologia que ha d'aplicar al servei que es vol contractar. Per altra banda, sí proposa un mecanisme de control de la qualitat del servei.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.5 PricewaterhouseCoopers PwC

La proposta de PricewaterhouseCoopers descriu la metodologia identificant un conjunt d'activitats del pla de qualitat però no dóna detall de què inclouen i com es faran. També es detalla l'assegurament de la continuïtat del servei identificant els riscos principals que són de rotació de personal i de les instal·lacions on es donen. Per altra banda, tot i que s'explica que hi haurà un quadre de comandament, no s'informa quin serà el procés de revisió i seguiment dels indicadors del quadre, per tant, no es detalla com es proposaran accions, mecanismes o altres elements que ajudin al compliment dels ANS.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.6 S2Grupo

La proposta de S2Grupo posa de relleu que per garantitzar el compliment del servei i la qualitat es basa en l'experiència del licitador i en les certificacions que poseeix ( ISO20000-1, ISO 27001, ISO 9000, ISO 14001, ISO 166002), però no concreta com impacten aquests elements a la millora del servei objecte de la contractació.

En quant a la millora contínua, proposa la metodologia PDCA (Plan-Do-Check-Control) que facilita el control i el seguimient de totes les activitats derivades de la prestació del servei, però no esmenta cap mecanisme de control i seguiment que utilitzarà per tal de garantir el compliment del servei, tampoc no esmenta com farà la gestió de riscos del servei.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.7 S21Sec

La proposta de S21Sec detalla el pla de qualitat del servei destacant la gestió dels recursos humans com aspecte rellevant per la qualitat del servei, indicant que això és així donat que bona part del servei s'oferirà a les oficines de la UOC. Aquest punt, no s'ajusta al que es demanat al Plec tècnic, punt 5.5. Localització física, on s'indica que el servei s'ha de prestar preferentment en les oficines del proveïdor.

El licitador subratlla que en els apartats 5.1.7 i 5.2 de la seva proposta, està detallat tant la gestió de la disponibilitat dels recursos humans, com la gestió de la rotació. Cap d'aquests dos apartats estan inclosos en el document de la proposta, per tant , no es poden avaluar.

En quant a mecanismes de control i seguiment, es proposa el seguiment dels indicadors per analitzar possibles desviacions, la incorporació d'un responsable que gestionarà la correcta execució i la priorització per garantir la qualitat i les reunions periòdiques.

En quant als riscos, s'explica que la detecció dels mateixos la farà l'equip de treball juntament amb el responsable de la UOC, també es proposa una classificació dels mateixos en riscos tècnics, de calendari o de cost.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.8 SAYTEL SERVICIOS INFORMÁTICOS

La proposta de SAYTEL SERVICIOS INFORMÁTICOS especifica el pla d'implantació, el pla de comunicació i els comitès de servei però no identifica ni detalla cap pla de qualitat que asseguri el compliment del mateix, ni descriu mecanismes de control més enllà que els comitès especificats al model de relació, ni identifica co es farà la gestió dels riscos que pot tenir el servei ni la seva mitigació.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

### 2.2.9 T-Systems

La proposta de T-Systems esmenta diferents metologies estàndards o reconegudes internacionalment com SM-Book (ITIL v3), PM-Book, Six Sigma, Quality Gates com a opcions per gestionar el servei o gestionar la qualitat però no explica com s'implementa o adapten aquesta metodologia al servei objecte de la licitació.

En quant a mecanismes de control i seguiment, per la fase del servei continuat, es proposen els informes de seguiment dels indicadors i de riscos i per presentar-los i validar-los en els comitès estratègics i tàctics, però no es proposa com es faria la gestió de riscos.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punts:** Si la proposta inclou:

Una descripció detallada de la metodologia que seguirà el proveïdor adjudicatari per tal de garantir el compliment del servei, especificant les diferents fases del servei així com el seu termini.

La proposta no inclou els mecanismes de control i seguiment que utilitzarà el proveïdor per tal de garantir el compliment del servei (mecanismes que ajudin al compliment dels ANS, accions especials per incidents repetitius, accions extraordinàries, detecció de riscos, etc.)

# 2.3. Eines (fins a 1 punt)

## 2.3.1 ERNST & YOUNG Global Limited

La proposta d'ERNST&YOUNG proposa una eina Quadre de comandament amb les dades dels informes de seguiment i els ANS, entre altres. La proposta indica que ofereix diferents interfícies del Quadre de comandament dirigida als diferents públics i també mostra exemples de diferents visualitzacions d'informes segons la visió més executiva o més tàctica o operativa. El disseny del quadre mostrat en la proposta evidencia que és una eina fàcil d'usar. També permet als responsables de la UOC, consultar en tot moment la situació del servei mostrant indicadors sobre vulnerabilitats, percentatge de risc, entre altres.

També proposen una eina de treball col·laboratiu, Slack, que s'integra a l'eina de Ticketing i el SIEM, aquesta proposta pot suposar una eficient comunicació entre els equips.

malgrat la idoneïtat d´aquestes solucions, la proposta no detalla la planificació de la posada en marxa de les mateixes.

El licitador ERNST&YOUNG, tal com es detalla anteriorment, aporta un conjunt d'eines idònies per a facilitar i millorar la prestació del servei però no incorpora la planificació per la posada en funcionament.

**0,5 punts:** La proposta inclou:

- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:

- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

## 2.3.2 Viewnext

La proposta de Viewnext no aporta cap eina addicional a les ja disponibles a la UOC, enfocades a facilitar i millorar la prestació del servei o la monitorització del mateix.

**0 punts:** Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

## 2.3.3 IThink UPC

La proposta d'IThink UPC detallen un conjunt d'eines i els beneficis que aporten a la gestió del servei. Entre altres, cal destacar, en primer lloc una eina de monitorització de l'estat del servei en temps real ,amb un plafó basat en Grafana, per tant, disposa d'una interfície gràfica que facilita l'ús i la visualització de la informació. Sobre la informació que conté, la proposta identifica els indicadors més rellevants que permetran avaluar l'acompliment dels ANS i també indicadors que permetran conèixer l'estat de la ciberseguretat a la UOC, entre altres, número de vulnerabilitats, indicadors ANS o número de tiquets oberts. Aquesta eina permet als responsables de la UOC, consultar en tot moment la situació del servei i dels anàlisis que es duen a terme.

També és rellevant que la proposta explica els mitjans per a la comunicació que posa a disposició del

servei i que es poden utilitzar per la gestió d'incidents, aquest mitjans són, entre altres : Informació de contacte per als membres de l'equip i altres persones dins i fora de l'organització, software xifrat per la comunicació entre els membres de l'equip, "war room" o espais/equips d'emmagatzematge segur per guardar evidències.

La proposta també inclou la posada en marxa de les eines especificades i que es duran a terme durant la fase transició, amb l´excepció del plafó, on la posada en marxa requerirà un calendari específic amb una duració de 6 setmanes.

El licitador IThink UPC, tal com es detalla anteriorment, aporta un conjunt d'eines idònies per a facilitar i millorar la prestació del servei.

**1 punts:** Si la proposta inclou:

- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.
- I, la idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- I el detall de la planificació prevista per la posada en funcionament de les eines.

### 2.3.4 (UTE) Opentrends + Cybernforce + Proficio

La proposta de la UTE Opentrends + Cybernforce + Proficio ofereix el portal ProView per visualitzar en temps real l'estat de la seguretat, aquest portal obté informació, entre altres, de les fonts del SIEM i de l'eina de ticketing, tanmateix, la proposta no informa com s'integra amb l'eina de ticketing que utiliza la UOC i , en quant a SIEM, es proposa migrar al SIEM en Cloud, proposta que la UOC no considera idònia ja que en el plec s'especifica que el SIEM que utilitzarà el servei és un equipament instal·lat i donant servei des del CPD de la UOC.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:

- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:

- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

### 2.3.5 PricewaterhouseCoopers PwC

Les eines proposades per PricewaterhouseCoopers són les s'han d'utilitzar per executar de manera automatitzada tasques dels serveis de ciberseguretat que formen part del servei regular.

No s'ofereix cap eina de monitorització o quadre de comandament de l'estat del servei en temps real, element necessari per fer el seguiment de la qualitat del servei.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:
- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

### 2.3.6 S2Grupo

La proposta de S2Grupo no aporta cap eina addicional a les ja disponibles a la UOC, enfocades a facilitar i millorar la prestació del servei o la monitorització del mateix.

**0 punts:** Si la proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### 2.3.7 S21Sec

La proposta de S21Sec ofereix un conjunt d'eines pròpies del proveïdor o de mercat que faciliten la detecció, escaneig o anàlisi de vulnerabilitats que són eines que s'utilitzen en el servei regular. També detalla la utilització d'un CA Service Desk però no explica com s'integrarà a l'eina que la UOC utilitza com a eina de tíqueting.

No s'ofereix cap eina de monitorització o quadre de comandament de l'estat del servei en temps real, element necessari per fer el seguiment de la qualitat del servei.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:
- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

### 2.3.8 SAYTEL SERVICIOS INFORMÁTICOS

La proposta de SAYTEL SERVICIOS INFORMÁTICOS aporta una eina de ticketing que utilitzarà l'equip del proveïdor i que s'integrarà a l'eina corporativa de ticketing de la UOC i altres eines que permeten realitzar de manera automatitzada els serveis de ciberseguretat que formen part del servei regular demanats en el plec tècnic. Aquestes eines ajuden a l'eficiència del servei però no permet al responsable del servei de la UOC fer el seguiment en temps real del servei .

No s'ofereix cap eina de monitorització o quadre de comandament de l'estat del servei en temps real, element necessari per fer el seguiment de la qualitat del servei.

El licitador SAYTEL SERVICIOS INFORMÁTICOS, tal com es detalla anteriorment, aporta un conjunt d'eines per gestionar les tasques del servei regular però cap eina addicional que faciliti i millori la

prestació del servei.

**0,5 punts:** La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:
- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

### 2.3.9 T-Systems

La proposta de T-Systems ofereix les eines del Portal de Seguretat i el Quadre de Comandament.
El Portal de Seguretat permet accedir de forma segura a la documentació, la planificació i la informació del servei, tenint una visió del nivell de risc i els indicadors definits. L'accés és remot online i permet generar informes bàsics a demanda de manera autònoma. Aquesta eina, per tant, proporciona facilitat d'extracció d'informació per l'anàlisi per part de la UOC.

Ell Quadre de comandament ofereix informació gràfica i a alt nivell de la situació del servei. Es permet establir llindars i objectius i es poden enviar alertes en cas que es superin aquests llindars. La proposta mostra exemples d'interfícies que evidencien la facilitat d´ús de l'eina.

Aquestes dues eines permetran a la UOC fer un seguiment en temps real del servei, analitzar el grau de risc i vulnerabilitats i alhora que avaluar com s'està oferint el servei mateix.

El licitador T-systems, tal com es detalla anteriorment, aporta un conjunt d'eines idònies per a facilitar i millorar la prestació del servei però no incorpora la planificació per la posada en funcionament**.**

**0,5 punts**: La proposta inclou:
- Una descripció de les funcionalitats del conjunt d´eines proposades, la facilitat d´ús i els serveis que es poden monitoritzar en temps real.

La proposta no inclou:
- La idoneïtat de les eines aportades, especificant el benefici que aporta als processos clau del servei.
- O, el detall de la planificació prevista de la posada en funcionament de les eines.

La puntuació total obtinguda al segon apartat, anomenat **GESTIÓ I GOVERNANÇA DEL SERVEI** és la següent:

| Taula de puntuació | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Puntuació màxima** | **5 punts** | **Ernst&Young** | **Viewnext** | **iThink UPC** | **UTE Opentrends Cybernforce Proficio** | **UTE PwC** | **S2 Grupo** | **S21Sec** | **Saytel** | **T-Systems** |
| 2. Gestió i Governança del servei | **5** | | | | | | | | | |
| 2.1. Model de relació | 1 | 1 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| 2.2. Metodologia, mecanismes de control i seguiment del servei | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2.3. Eines | 1 | 0,5 | 0 | 1 | 0,5 | 0,5 | 0 | 0,5 | 0,5 | 0,5 |
| | | 4,5 | 1,5 | 2,5 | 2 | 2 | 1,5 | 2 | 2 | 2 |

## 3. Fases de la prestació del servei (fins a 5 punts)

## 3.1. Auditoria i Transformació (fins a 2 punts)

### 3.1.1 ERNST & YOUNG Global Limited

En primer lloc ERNST & YOUNG Global Limited presenta el pla de transició amb un complert detall de les fases (adquisició de coneixement, auditoria, planificació de la transformació, pla d'activació del servei, finalització de la transició, pla de riscos de la transició). Per cada fase, el licitador presenta ordenadament els objectius, les tasques, les entrades i les sortides. Per últim presenta un quadre amb els recursos assignats per perfil per cada fase en %, sense valors absoluts.

ERNST & YOUNG fa un detall adequat de fites i processos en línia a les prescripcions tècniques recollides als punts 6.1. i 6.2. del plec tècnic. També presenta els recursos i perfils que assignarà a cada fase però només en %, cosa que no permet valorar la idoneïtat de la proposta. També es troba a faltar un calendari justificat per l'assoliment dels objectius.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.2 Viewnext

Viewnext a la seva proposta presenta les tasques a desenvolupar durant l'auditoria i la transformació. Per últim expressa la intenció de pactar amb UOC els models operatiu i de gestió del servei sense donar cap altre informació. No hi ha detalls de com portarà a terme la transformació ni dona cap informació sobre calendari ni recursos.

Viewnext presenta una proposta on detalla les fites i processos en línia a les prescripcions tècniques recollides als punts 6.1. i 6.2. del plec tècnic.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.3 IThink UPC

IThink UPC fa una proposta basada en les dues fases (auditoria i transformació). Detalla els objectius a assolir amb la fase d'auditoria. Seguidament presenta el pla de transferència i per últim la fase de transformació. Per cada punt fa una descripció detallada de les tasques, recursos i perfils assignats així com la metodologia i el calendari que aplicarà. Tota la proposta està adaptada als requeriments recollits als punts 6.1. i 6.2. del plec tècnic i defineix amb precisió els perfils que executaran cada tasca.

La proposta de IThink UPC inclou de forma detallada els processos i fites per assolir aquesta fase i que estan en línia amb els requeriments tècnics, amb el calendari, la metodologia i els recursos i perfils que assignarà a cada tasca.

**2 punts:** La proposta inclou:

Una descripció detallada de la proposta tècnica, on s´inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria i transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s´inclou:

La metodologia utilitzada
El nombre de recursos que es dedicaran així com els seus perfils.

### 3.1.4 (UTE) Opentrends + Cybernforce + Proficio

Opentrends + Cybernforce + Proficio a la seva proposta presenta les tasques a desenvolupar durant l'auditoria fent èmfasi en la criticitat dels actius i en l'anàlisi de riscos. Seguidament relaciona les accions a realitzar per la transformació amb dos apartats: Pla d'implantació i infraestructures i transferència de coneixement. Tant a l'auditoria com a la transformació dona el temps estimat per cobrir aquests dos apartats..

La proposta de Opentrends + Cybernforce + Proficio inclou una descripció bàsica de fites, processos

i calendari en línia amb els requeriments dels punts 6.1. i 6.2. del plec tècnic però no inclou cap informació sobre metodologia, recursos ni perfils.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.5 PricewaterhouseCoopers PwC

PricewaterhouseCoopers PwC presenta una planificació d'aquesta fase en cinc apartats (anàlisi inicial, model de govern, pla d'acció, adquisició i estabilització). Per cadascun dels apartats dona informació sobre les activitats a realitzar, la metodologia a utilitzar i els resultats esperats. No hi ha informació sobre els recursos en cap dels apartats. Presenta un calendari basat en 4 mesos de duració que no concorda amb la limitació de 3 mesos requerida al plec tècnic. Respecte als recursos és limita a involucrar al coordinador del servei i un perfil d'auditor en seguretat però sense relacionar-los amb funcions ni activitats i no es fa al·lusió a cap perfil tècnic.

La proposta de PricewaterhouseCoopers PwC inclou detall suficient dels processos i fites que permetin assolir la fase d´auditoria i transformació segons les prescripcions dels apartats 6.1. i 6.2. del plec tècnic, però es troba a faltar detalls i coherència sobre els recursos i perfils que dedicarà i del calendari que s'aplicarà.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.6 S2Grupo

S2Grupo comença presentant un pla d'auditoria detallat però fonamentalment centrat en la detecció de vulnerabilitats deixant els altres àmbits sense comentar. Seguidament passa a descriure el procés de transformació del servei a nivell teòric, ens descriu com han de ser els procediments segons les metodologies i estàndards del mercat. Seguidament dona informació detallada de les qualitats a les que S2grupo es compromet sobre els procediments a elaborar en línia amb el demanat al plec tècnic. No hi ha cap referència als recursos o calendari que aplicarà.

La proposta de S2Grupo inclou detalls de processos i fites detallats i en línia amb als requeriments

recollits als punts 6.1. i 6.2. del plec tècnic, però és una proposta parcial, basada en la detecció de vulnerabilitats en el cas de l'auditoria i en els procediments en el cas de la transformació. Tampoc dona cap informació sobre recursos i perfils a assignar ni calendari d'execució.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.7 S21Sec

S21Sec relaciona a la seva proposta les àrees de l'empresa que estaran implicades però sense concretar l'abast d'aquesta implicació, anteriorment ha indicat que dedicarà un esforç de 320h a aquestes fases però sense donar més detall. Seguidament descriu amb detall el procés d'auditoria amb els objectius, tasques i lliurables. Seguidament presenta la fase de definició del pla de transformació i la presentació de resultats final on també es detallen els objectius, les tasques i els lliurables. Falten detalls de com s'executarà el pla. No dona informació sobre els recursos que assignarà a cada fase.

S21Sec presenta una proposta ben detallada en quant a mètode i fites a aconseguir en línia amb els requeriments tècnics recollits als punts 6.1. i 6.2 del plec tècnic, però falta detall en quan al calendari a seguir, i els recursos i perfils que assignarà en la seva execució.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

#### 3.1.8 SAYTEL SERVICIOS INFORMÁTICOS

SAYTEL SERVICIOS INFORMÁTICOS fa una proposta basada en les dos fases principals (auditoria i transformació). A l'auditoria defineix les fites i projectes principals (adquisició del coneixement i preparació tecnica) on fa una descripció detallada de la informació i coneixement que Saytel requerirà per part de UOC. Per la fase de transformació, igualment defineix les fites i projectes claus on descriu com ha de ser el traspàs dels serveis, quin anàlisi de riscos es portarà a terme i quin pla de qualitat es proposa. Per les dues fases presenta un calendari suficientment detallat i coherent amb els requeriments.

Saytel presenta una proposta suficientment detallada respecte a metodologia, processos i fites per

assolir aquesta fase en línia amb els requeriments tècnics recollits als punts 6.1. i 6.2 del plec tècnic, però no dona informació sobre els recursos ni perfils que assignarà a la transició.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

### 3.1.9 T-Systems

T-Systems presenta quatre etapes per l'execució de l'auditoria i la transformació (inici, planificació, control de la transformació, tancament). Per cada etapa dona una relació de les accions bàsiques que portarà a terme i amb el resultat i/o lliurable de cada acció sense entrar en detalls tècnics. Es troba a faltar informació sobre organització i el nombre de recursos que dedicarà i amb quins perfils.

El licitador defineix uns processos i calendari coherent amb les prescripcions tècniques recollides als punts 6.1. i 6.2 del plec tècnic, però es troben a faltar detalls sobre la metodologia que farà servir i no aporta informació sobre organització ni recursos i perfils que farà servir en aquesta fase.

**Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.**

**1 punt.** La proposta inclou:
Una descripció detallada de la proposta tècnica, on s'inclou:

La definició dels processos i fites que permetin assolir la fase d´auditoria transformació.
Calendari proposat que permeti l´assoliment d´aquesta fase en el termini establert en el PPT
I, una descripció detallada de la proposta organitzativa, on s'inclou la metodologia utilitzada, però no inclou el nombre de recursos que es dedicaran ni els seus perfils.

## 3.2. Servei regular (fins a 1 punt)

### 3.2.1 ERNST & YOUNG Global Limited

ERNST & YOUNG Global Limited presenta una relació de mecanismes per assegurar la qualitat i la millora contínua basat en quatre processos (Quality plan, quality assurance, quality control, continuous improvement) definint l'activitat, la periodicitat i en quin entorn s'executarà. No entra en detalls tècnics concrets sobre l'assegurament de l'estabilitat ni la detecció de riscos ni tampoc sobre els recursos involucrats.

El licitador presenta un pla de millora contínua coherent que està en línia amb els requeriments demanats i els prescripcions tècniques de l'apartat 6.3 del plec tècnic, però es troben a faltar els detalls

tècnics sobre els mecanismes que establirà per poder garantir la idoneïtat dels mateixos ni com evidenciarà els resultats del pla de millora.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:

Una proposta de millora contínua, on es detallen els mecanismes necessaris per tal de garantir l'estabilitat del servei

La proposta no inclou:

Els mecanismes per tal d'identificar una detecció temprana de riscos

Ni els mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.2 Viewnext

Viewnext a la seva proposta descriu les activitats que portarà a terme durant la fase regular sense que hi hagi cap proposta de millora contínua ni cap detall sobre els mecanismes demanats. Seguidament passa a relacionar els requeriments per part de  i UOC pel correcte tractament de les dades i la propietat intel·lectual que tampoc és el que es demana en l'apartat.

El licitador no presenta cap mecanisme concret per assegurar l'estabilitat del servei ni per la detecció de riscos.

**0 punts:** La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### 3.2.3 IThink UPC

IThink UPC defineix els objectius de la fase regular i els relaciona amb el pla de millora continua que passa a descriure. La seva proposta de millora continua inclou la relació de mecanismes destinats a assegurar l'estabilitat del servei i la detecció de riscos, incorporant els mecanismes que permetran fer el seguiment del propi pla. El coordinador del servei serà la principal figura per la gestió del pla de millora i relaciona les accions que portarà a terme per la seva execució i seguiment. Per últim presenta un pla de formació de l'equip assignat per garantir la seva preparació i capacitació al llarg del servei.

Per tot l'exposat anteriorment, es considera que la proposta del proveïdor dona compliment de forma detallada a tots els punts que es valoren en aquest apartat.

**1 punt:** La proposta inclou una proposta de millora contínua completa detallant:

Els mecanismes necessaris per tal de garantir l'estabilitat del servei

Els mecanismes per tal d'identificar una detecció temprana de riscos

Mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.4 (UTE) Opentrends + Cybernforce + Proficio

Opentrends + Cybernforce + Proficio es limita a relacionar els punts a pactar amb UOC per l'estabilització del servei però no proposa cap acció concreta, i no descriu cap model de millora contínua ni concreta cap mecanisme de continuïtat d'estabilitat ni de control de riscos com es demana en aquest apartat. Tampoc apareix cap mecanisme de seguiment del pla de millora.

**0 punts:** La proposta és manifestament incompleta, no cobrint cap dels elements especificats en aquest apartat.

### 3.2.5 PricewaterhouseCoopers PwC

PricewaterhouseCoopers PwC presenta un pla de qualitat basat en la documentació dels punts que considera més crítics. A continuació defineix un pla de continuïtat del servei basat en com s'afrontaran les substitucions del personal assignat al servei i com afrontar els problemes d'accés als llocs de treball. No hi ha informació sobre mecanismes concrets d'estabilitat sobre el servei demanat. Per últim parla dels mecanismes de control però només a nivell conceptual que es basarà en auditories i informes forenses.

La proposta de PricewaterhouseCoopers PwC sobre un pla de millora contínua està basat en intencions a nivell conceptual sense detallar cap mecanisme d'estabilitat ni de control de riscos concret relacionat amb el servei demanat. Tampoc hi ha cap mecanisme definit per evidenciar els resultats del pla de millora.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:

Una proposta de millora contínua, on es detallen els mecanismes necessaris per tal de garantir l'estabilitat del servei

La proposta no inclou:

Els mecanismes per tal d'identificar una detecció temprana de riscos

Ni els mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.6 S2Grupo

En aquest apartat S2Grupo presenta la definició dels processos del servei a un nivell teòric on la única informació rellevant que dona sobre aquest servei són les entrades i sortides d'aquests processos i qui serà el responsable de cada procés. La proposta no conté un model de millora contínua clar.

S2Grupo presenta la definició dels processos del servei sense informació rellevant sobre els mecanismes d'estabilitat, de detecció de riscos ni del seguiment del pla de millora.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:

Una proposta de millora contínua, on es detallen els mecanismes necessaris per tal de garantir l'estabilitat del servei

La proposta no inclou:

Els mecanismes per tal d'identificar una detecció temprana de riscos

Ni els mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.7 S21Sec

S21Sec presenta un pla de millora detallat on fa propostes concretes relacionades amb el servei que ocupa incloent els mecanismes per garantir l'estabilitat, els mecanismes de detecció de riscos i els mecanismes pel seguiment del propi pla descrivint accions concretes adequades pel servei demanat i en línia als requeriments dels apartats 6.2 i 6.3 del plec tècnic. El pla de millora es basa en la presentació regular (trimestral) de propostes de millora a partir d'un equip expert coordinat pel responsable del servei, el compromís de dedicar el 10% dels recursos tècnics a l'execució del pla i el seguiment del pla a través d'un quadre de comandament per poder fer el seguiment del pla.

S21Sec presenta mecanismes per garantir l'estabilitat, detecció de riscos i seguiment del pla de millora suficientment descrits i en línia amb les prescripcions tècniques.

**1 punt:** La proposta inclou una proposta de millora contínua completa detallant:
Els mecanismes necessaris per tal de garantir l'estabilitat del servei
Els mecanismes per tal d'identificar una detecció temprana de riscos
Mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.8 SAYTEL SERVICIOS INFORMÁTICOS

SAYTEL SERVICIOS INFORMÁTICOS presenta una proposta de millora contínua basada en uns objectius estratègics que inclouen mecanismes d'estabilitat i detecció de riscos però a un nivell molt generalista sense adaptar-los al servei concret. També inclou un pla de formació continua per l'equip del servei però sense concretar suficientment el seu abast.

La proposta de millora contínua del licitador presenta mecanismes d'estabilitat i detecció de riscos a un nivell bàsic sense entrar en els detalls de com seran aplicats sobre aquest servei. No es descriuen els mecanismes per tal d'evidenciar els resultats de l'aplicació del pla de millora.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat.

**0,5 punts:** La proposta inclou:
Una proposta de millora contínua, on es detallen els mecanismes necessaris per tal de garantir l'estabilitat del servei
La proposta no inclou:
Els mecanismes per tal d'identificar una detecció temprana de riscos
Ni els mecanismes necessaris per evidenciar els resultats d´aplicació del pla de millora.

### 3.2.9 T-Systems

T-System ofereix la utilització de la metodologia estàndard bimodal "clàssica i/o àgil" i fa una petita descripció teòrica d'aquestes metodologies i presenta uns gràfics sobre la implementació de Scrum a T-systems on no hi ha cap mecanisme per garantir l'estabilitat del servei que és el que es demana en aquest apartat. Tot el que presenta és teòric i no hi ha una proposta de millora contínua relacionada amb el servei demanat.

El licitador no presenta cap mecanisme concret per assegurar l'estabilitat del servei ni per la detecció de riscos.

**0 punts:** La proposta és manifestament incompleta, no cobrint cap dels elements especificats en

aquest apartat.

## 3.3. Devolució del servei (fins a 2 punts)

### 3.3.1 ERNST & YOUNG Global Limited

En primer lloc ERNST & YOUNG Global Limited presenta la metodologia de devolució basada en cinc fases (definició del model de governança, transferència del coneixement, cessió gradual del servei, període de garantia, gestió dels riscos). Per cada fase defineix els objectius i les tasques a realitzar. Seguidament presenta un quadre amb les fases i els recursos assignats a cadascuna en %, sense valors absoluts, la qual cosa no permet valorar la idoneïtat de la proposta. En la proposta tampoc es fa menció dels informes que s´entregaran en aquesta fase. Per últim presenta un calendari d'execució de les fases.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat.

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:

- Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
- Ni la durada compromesa de l´equip de treball.
- Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.2 Viewnext

Viewnext proposa fer servir la metodologia TTM que es podrà invocar de forma ordinària o extraordinària. No presenta com s'aplica aquesta metodologia al servei que ocupa. Finalment fa una relació d'activitats a realitzar durant la fase de devolució però sense donar informació concreta de cadascuna ni com es concreta pel servei demanat.

La proposta de Viewnext no inclou els mitjans als que es comprometrà durant la fase, ni de la documentació que lliurarà.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:

- Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
- Ni la durada compromesa de l´equip de treball.
- Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.3 IThink UPC

IThink UPC en primer lloc presenta els objectius a assolir a la fase de devolució. A continuació dona els compromisos per tal d'assolir aquests objectius incloent les tasques, recursos i perfils involucrats. Seguidament fa una descripció de la metodologia que seguirà basada en cinc etapes (Inici de la devolució, Lliurament de la documentació, Traspàs de l'experiència i organització de la formació, Prestació del servei amb equips mixtes, Fi de la Prestació del servei i traspàs de la responsabilitat) que està en línia amb els requeriments de l'apartat 6.4 del plec tècnic. Per cadascuna, el licitador descriu clarament el seu contingut detallant els mitjans, perfils i compromisos. Per últim descriu el pla de seguiment i els lliurables de la fase de devolució del servei.

IThink UPC fa una descripció detallada de la metodologia corresponent a la fase de devolució, dels mitjans compromesos, identificant la idoneïtat de l´equip proposat amb la durada compromesa de l'equip, així com el detall de lliurament d'informes cobrint tots els àmbits i processos del servei.

**2 punts:** La proposta inclou:

Una descripció detallada de la metodologia corresponent a la fase de devolució.
I els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
I la durada compromesa de l´equip.
I entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.4 (UTE) Opentrends + Cybernforce + Proficio

Opentrends + Cybernforce + Proficio a la seva proposta presenta, en primer lloc, en que ha de consistir la devolució a nivell conceptual. Seguidament defineix les activitats que portarà a terme durant la devolució agrupades per: planificació, procediments i documentació i transferència de coneixement. En cap cas dona informació sobre els compromisos sobre els mitjans ni dels informes que lliurarà.

Tot i que Opentrends + Cybernforce + Proficio dona una relació d'activitats a realitzar no dona cap informació sobre els compromisos i duració dels mitjans assignats o el lliurament d'informes.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:

Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l´equip de treball.
Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.5 PricewaterhouseCoopers PwC

PricewaterhouseCoopers PwC presenta una descripció adequada de les activitats que realitzarà durant la fase de devolució en línia amb els requeriments del servei de l'apartat 6.4 del plec tècnic. A continuació es limita a confirmar qui serà responsable dels ANS tal com demana el plec tècnic i acaba nombrant els informes que presentarà trobant-se a faltar una descripció del contingut dels mateixos. La proposta tampoc inclou una descripció dels mitjans compromesos per la devolució i del contingut

dels informes que lliurarà.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances de detall donant compliment de forma parcial als punts valorats en aquest apartat

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:
Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l´equip de treball.
Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.6 S2Grupo

En aquest apartat S2Grupo defineix a nivell bàsic la informació que considera necessària per l'execució d'aquesta fase i defineix amb detall el seguiment de l'execució basat en les accions de dos comitès (tàctic i operatiu). Per cada comitè el licitador detalla les accions a realitzar, la seva periodicitat i les persones que assistiran, en las que apareix el perfil de responsable de la finalització sense donar més informació sobre aquest perfil. Es troba a faltar en la proposta del proveïdor una descripció sobre els recursos i compromisos en l'execució d'aquesta fase.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:
Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l´equip de treball.
Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.7 S21Sec

S21Sec presenta una estratègia de devolució basada en sis elements de treball (identificació de medis, identificació de rols i responsabilitats, identificació de documentació, acompanyament, supervisió de les tasques de l'entrant, fase final i lliurament del servei). De cadascun fa un detall suficient de les tasques a realitzar. No dóna informació sobre mitjans a assignar ni compromisos en l'execució d'aquesta fase.

Per tot l'exposat anteriorment, la proposta del proveïdor té mancances detall donant compliment de forma parcial als punts valorats en aquest apartat

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:
Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l'equip de treball.

Ni la entrega d'informes que cobreixin tots els àmbits i processos del servei.

### 3.3.8 SAYTEL SERVICIOS INFORMÁTICOS

SAYTEL SERVICIOS INFORMÁTICOS presenta una proposta basada en tres fases (planificació, devolució del servei, lliurament del servei) en la que es relacionen les tasques, la informació a lliurar i l'equip que les executarà. No hi ha informació sobre compromisos en els mitjans i recursos involucrats.

La proposta de Saytel presenta una descripció detallada de la metodologia en línia amb els requeriments dels apartats 6.3 i 6.4 del plec tècnic, fa una descripció molt bàsica dels informes a lliurar i no inclou els mitjans compromesos per la devolució, ni identifica la idoneïtat de l´equip proposat ni la durada compromesa de l'equip de treball.

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:

Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l´equip de treball.
Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

### 3.3.9 T-Systems

T-Systems presenta un pla de devolució que està alineat amb els requeriments tècnics dels apartats 6.3 i 6.4 del plec tècnic. En primer lloc descriu la metodologia que farà servir per establir el pla de devolució i el model de relació. A continuació presenta una planificació amb les diferents etapes d'aquesta fase amb la seva descripció. Per últim dona el criteri de finalització de la devolució amb el lliurament d'un document de tancament relacionant el seu contingut. No hi han suficients detalls sobre els recursos assignats a la devolució, només concreta la dedicació d'un tècnic especialista en shadowing al darrer mes de la devolució però sense concretar la seva dedicació, tampoc concreta la dedicació de la resta de l'equip tècnic.

El licitador fa una proposta suficientment detallada en relació a la metodologia i a la informació lliurada que està en línia amb el demanat al plec tècnic però falta informació sobre els recursos que destinarà i la durada dels mateixos.

**1 punt:**
La proposta inclou: Una descripció detallada de la metodologia corresponent a la fase de devolució.
La proposta no inclou:

Els mitjans compromesos per la devolució, identificant la idoneïtat de l´equip proposat.
Ni la durada compromesa de l´equip de treball.
Ni la entrega d´informes que cobreixin tots els àmbits i processos del servei.

La puntuació total obtinguda al segon apartat, anomenat **FASES DE PRESTACIÓ DEL SERVEI** és la següent:

| **Taula de puntuació** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Puntuació màxima** | **5 punts** | **Ernst&Young** | **Viewnext** | **iThink UPC** | **UTE Opentrends Cybernforce Proficio** | **UTE PwC** | **S2 Grupo** | **S21Sec** | **Sayt el** | **T-Systems** |
| 3. Fases de Prestació del Servei | **5** | | | | | | | | | |
| 3.1. Auditoria i Transformació | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3.2. Servei Regular | 1 | 0,5 | 0 | 1 | 0 | 0,5 | 0,5 | 1 | 0,5 | 0 |
| 3.3. Devolució del servei | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| | | 2,5 | 2 | 5 | 2 | 2,5 | 2,5 | 3 | 2,5 | 2 |

# Puntuació final

Per tot l'exposat, es conclou que la puntuació total obtinguda pels licitadors en el Sobre núm. 2 és la següent:

| Taula de puntuació | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Puntuació màxima | 40 punts | Ernst&Young | Viewnext | iThink UPC | UTE Opentrends Cybernforce Proficio | UTE PwC | S2 Grupo | S21Sec | Saytel | T-Systems |
| 1. Proposta de prestació del servei | 30 | | | | | | | | | |
| 1.1. Detecció, anàlisi i gestió de vulnerabilitats | 6 | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 3 | 1 | 1 | 3 | 1 |
| B. Recursos assignats | 3 | 3 | 3 | 3 | 0 | 3 | 1 | 1 | 3 | 1 |
| 1.2. Gestió i resposta a incidents de seguretat de la informació CSIRT | 6 | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 3 | 1 | 1 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 3 | 1 | 1 | 3 | 1 |
| 1.3. Anàlisi de malware | 6 | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 1 | 1 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| 1.4. Anàlisi forense | 6 | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 1 | 0 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| 1.5. Manteniment, revisió, administració i reporting de la infraestructura de seguretat de la UOC | 6 | | | | | | | | | |
| A. Solució proposada | 3 | 3 | 1 | 3 | 1 | 1 | 0 | 0 | 1 | 1 |
| B. Recursos assignats | 3 | 3 | 1 | 3 | 0 | 1 | 1 | 1 | 3 | 1 |
| TOTAL PUNT 1 | **30** | **30** | **12** | **30** | **5** | **18** | **9** | **8** | **22** | **10** |
| 2. Gestió i Governança del servei | 5 | | | | | | | | | |
| 2.1. Model de relació | 1 | 1 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| 2.2. Metodologia, mecanismes de control i seguiment del servei | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2.3. Eines | 1 | 0,5 | 0 | 1 | 0,5 | 0,5 | 0 | 0,5 | 0,5 | 0,5 |
| **TOTAL PUNT 2** | **5** | **4,5** | **1,5** | **2,5** | **2** | **2** | **1,5** | **2** | **2** | **2** |
| 3. Fases de Prestació del Servei | 5 | | | | | | | | | |
| 3.1. Auditoria i Transformació | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3.2. Servei Regular | 1 | 0,5 | 0 | 1 | 0 | 0,5 | 0,5 | 1 | 0,5 | 0 |
| 3.3. Devolució del servei | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| **TOTAL PUNT 3** | **5** | **2,5** | **2** | **5** | **2** | **2,5** | **2,5** | **3** | **2,5** | **2** |
| | | 37 | 15,5 | 37,5 | 9 | 22,5 | 13 | 13 | 26,5 | 14 |

Finalment, la puntuació obtinguda pels licitadors ordenada en ordre decreixent és la següent:

| | |
|---|---|
| **Ithink UPC** | **37,5 Punts** |
| **ERNST & YOUNG Global Limited** | **37 Punts** |
| **SAYTEL SERVICIOS INFORMÁTICOS** | **26,5 punts** |
| **PricewaterhouseCoopers PwC** | **22,5 punts** |
| **Viewnext** | **15,5 punts** |
| **T-Systems** | **14 punts** |
| **S21Sec** | **13 punts** |
| **S2Grupo** | **13 punts** |
| **(UTE) Opentrends + Cybernforce + Proficio** | **9 punts** |

Barcelona, 26 de Febrer de 2020

Signat,

Ricard Mateu Guasch
Director Projectes i Aplicacions

Eloi Serra Saura
Director Àrea Serveis Generals