SEIDOR

Human focused
Technology experts

Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya

PROPOSTA TÈCNICA

Expedient 2024.01 LOT 36

INDEX

1. INTRODUCCIÓ

El Grup SEIDOR és una multinacional catalana de consultoria tecnològica, fundada el 1982, present en 45 països i amb mes de 9.000 col·laboradors (uns 1.500 a Catalunya). Està format per un grup d'empreses especialitzades en camps tecnològics, que acrediten una solvència tècnica i experiència de servei per impulsar la innovació i la digitalització com la millor via per a la transformació de les organitzacions.

SEIDOR impulsa la competitivitat i la transformació de les organitzacions des de les oportunitats que presenten les tecnologies i el coneixement de negoci, amb focus sempre en el valor del que és humà i compromesos amb el talent i el desenvolupament social.

A través de les nostres activitats, accions i aliances estratègiques, contribuïm a la consecució dels Objectius de Desenvolupament Sostenible (ODS). Destaquem com a elements de valor afegir les següents iniciatives corporatives:

Drets Humans

Aprovisionament de recursos a col·lectius més desfavorits. Col·laboració amb institucions educatives per a reduir la bretxa digital i facilitar l'accés formatiu a col·lectius amb limitada capacitat econòmica

Treball

Col·laboració amb institucions per a afavorir i potenciar la diversitat, equitat i inclusió. Desenvolupament de comunitats per a l'ocupabilitat. Actualització del Pla d'Igualtat Corporatiu

Medi ambient – NET ZERO

Neutralitat en el nostre impacte en el medi ambient. Participació en projectes que fomentin l'economia circular. Participació en grups de treball de Sostenibilitat mediambiental

Gestió ètica

Accions de conscienciació entorn de la ciberseguretat, gestió de riscos i oportunitats i finances corporatives sostenibles orientades als ODS

A continuació, ens complau presentar la memòria tècnica que considerem mes adient, detallant els processos, eines i metodologies de cara a complir amb els requisits plantejats per Consorci Català pel Desenvolupament Local (CCDL) respecte els serveis de Ciberseguretat. Considerem aquests serveis una part fonamental de l'activitat del CCDL, per fer front al compliment normatiu i el disseny de solucions de seguretat que millorin la vida dels Ciutadans.

Tanmateix, des de SEIDOR s'aposta per una integració laboral completa tant per introduir perfils amb discapacitat com apropar els professionals mes joves al món de la Ciberseguretat. Es per això que tenim conveni de col·laboració tant amb la fundació GOODJOB com ENTI-UB per garantir i demostrar el compromís que té SEIDOR amb la integració laboral juntament amb altres convenis de col·laboració amb altres entitats i universitats.

La present proposta tècnica respon als requeriments establerts en el Plec de Prescripcions Tècniques corresponent al Lot 36, amb l'objectiu de dotar els ens locals adherits d'uns serveis de ciberseguretat moderns, eficients i alineats amb els estàndards més exigents de la ciberseguretat.

2. PRESTACIÓ 172. SERVEI D'ASSESSORIA:

2.1 AUDITORIA I CONSULTORIA INICIAL:

L'auditoria i consultoria inicial constitueixen el punt de partida essencial per a qualsevol acció de millora i adequació en matèria de ciberseguretat. El nostre enfocament es basa en una aproximació sistemàtica, estructurada i metodològica per tal de realitzar una radiografia precisa de l'estat de seguretat de la infraestructura tecnològica de l'entitat, identificar riscos i proposar accions correctores.

Aquest procés s'alinea principalment amb les bones pràctiques establertes pel Reial decret 311/2022, que regula l'Esquema Nacional de Seguretat (ENS), així com amb les altres normatives aplicables com poden ser NIS2 o RGPD i el model MAGERIT per a l'anàlisi de riscos.

Objectius de l'auditoria:

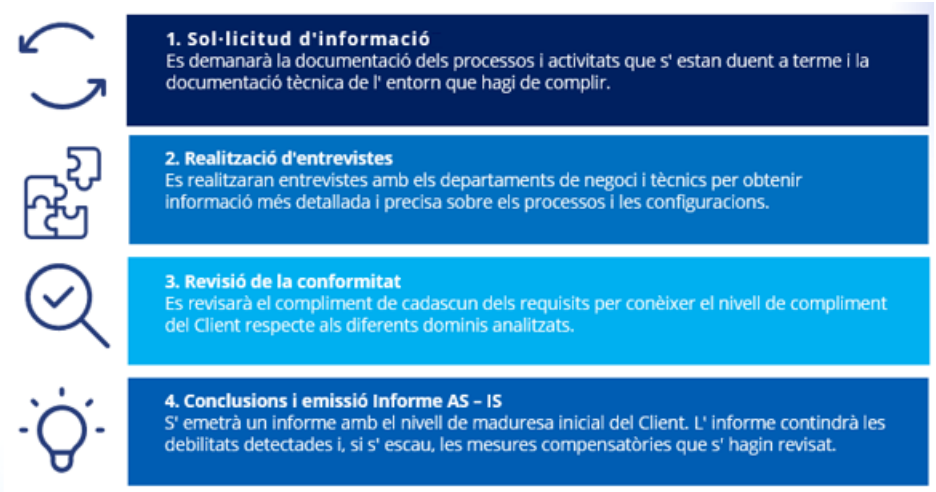
- Determinar el grau de maduresa actual en matèria de ciberseguretat.
- Identificar vulnerabilitats i mancances de seguretat tècnica i organitzativa.
- Establir una línia base a partir de la qual elaborar un pla de millora realista i executable.

Metodologia general aplicada:

L'auditoria es desplega a través d'un conjunt de fases que permeten una avaluació holística i adaptada a la realitat de cada entitat local.

Aquesta auditoria estarà basada en els models oficials i adaptada a cada entitat, de manera que sigui eficient. Aquesta part l'aconseguim mitjançant l'ús del CCN-STIC 808 (Verificació del compliment ENS) com a model principal, junt amb altres específics que poden ser aplicables en funció del ecosistema tecnològic del client. Per exemple, la "Guia de Seguridad de las TIC CCN-STIC 885A (Guia de configuració segura para Office 365)" si l'entitat disposa d'aquesta plataforma.

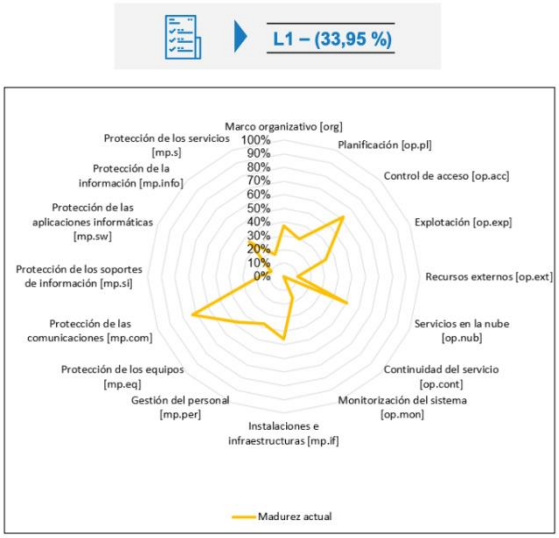
Aquest anàlisi inicial, de manera general, constarà de les següents fases:



Amb aquesta metodologia, es cobriran tots els aspectes de control que determina la normativa, inclosa la vessant tècnica mitjançant el catàleg de controls tècnics del ENS que contemplen de manera detallada aspectes com les copies de seguretat, controls d'accessos, protecció de les comunicacions, correu electrònic, xifrat, etc.

Aquesta auditoria generarà com a lliurable de valor un resum executiu (veure exemple) amb la maduresa estimada per cada àrea de control, junt amb un pla de millora (apartat següent) que permetrà a l'entitat evolucionar cap a una maduresa òptima, sempre adaptada a la seva naturalesa i requisits.

Controles	Madurez actual
Marco organizativo [org]	**37,50%**
Marco operacional [op]	**28,76%**
Planificación [op.pl]	30,00%
Control de acceso [op.acc]	61,67%
Explotación [op.exp]	33,00%
Recursos externos [op.ext]	10,00%
Servicios en la nube [op.nub]	50,00%
Continuidad del servicio [op.cont]	0,00%
Monitorización del sistema [op.mon]	16,67%
Medidas de protección [mp]	**35,59%**
Instalaciones e infraestructuras [mp.if]	45,71%
Gestión del personal [mp.per]	37,50%
Protección de los equipos [mp.eq]	47,50%
Protección de las comunicaciones [mp.com]	72,50%
Protección de los soportes de información [mp.si]	18,00%
Protección de las aplicaciones informáticas [mp.sw]	10,00%
Protección de la información [mp.info]	36,00%
Protección de los servicios [mp.s]	17,50%



2.2 PLA DE MILLORA:

El Pla de Millora constitueix la peça clau que transforma l'anàlisi tècnica i normativa realitzada durant l'auditoria en un conjunt estructurat d'actuacions prioritzades, realistes i adaptades al context de cada entitat local. Aquest pla es dissenya com un full de ruta executiu, que permet a l'organització avançar cap a una infraestructura més segura, resilient i conforme amb el marc regulador.

Aquest Pla no es limita a l'àmbit tècnic, sinó que contempla tant les dimensions tecnològiques, organitzatives i procedimentals, amb especial atenció al compliment del Reial decret 311/2022 (ENS) i de la directiva NIS2 per a entorns de serveis essencials o crítics.

Objectius principals:

- Definir accions concretes i prioritzades per assolir el compliment segons la categoria del sistema.
- Millorar el nivell de protecció davant ciberamenaces reals, amb especial èmfasi en aspectes de actualitat com el ransomware, el phishing i la fuita de dades.
- Guiar l'evolució de l'entorn cap a un model de seguretat gestionada i sostenible, amb capacitat de resposta i millora contínua.

Metodologia general aplicada:

En SEIDOR, aquest pla de millora o adequació contempla un seguit d'activitats perfectament definides, que segueixen les directrius de l'ENS i permeten acostar els clients cap a una maduresa òptima. De manera general, aquest pla contemplarà les següents activitats clau:

Pla de millora

Tasques:

La Certificació i Conformitat amb l'ENS comporta l'elaboració prèvia d'un Pla d'Adequació i millora que inclogui les fases prèvies següents:

A. **Identificació de l'abast del sistema.**
B. **Categorització del sistema.**
C. **Declaració d'Aplicabilitat provisional.**
D. **Anàlisi de riscos.**
E. **Declaració d'Aplicabilitat definitiva.**
F. **Política de seguretat.**

Descripció:

A. Identificació de l'abast del sistema. Establir l'abast dels sistemes d'informació inclosos en l'adequació. Es tracta de modelar l'arquitectura de serveis prestats pel client dins de l'àmbit de l'ENS per posteriorment identificar els sistemes IT que suporten aquests serveis de negoci.

B. Categorització del sistema. Valoració de les necessitats de seguretat en base a la disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat dels serveis i informació. La categorització és important perquè marca l'aplicació dels controls.

C. Declaració d'aplicabilitat provisional**.** Definir el document de la Declaració d'Aplicabilitat, en l'àmbit de l'ENS, en el qual es formalitza la relació de mesures de seguretat que resulten d'aplicació al sistema d'informació de què es tracti, conforme a la seva categoria. En base als resultats de l'auditoria inicial es determinarà el punt de sortida i l'acció detallada (full de ruta) per tal d'evolucionar cap a una infraestructura mes segura, incloent detalls tant de maquinari com de programari necessaris o recomanats i una estimació de l'esforç que comportaria aquesta recomanació.

D. Anàlisi de riscos**.** Identificar els riscos potencials i residuals en un sistema d'informació i comunicacions mitjançant una metodologia d'anàlisi i gestió de riscos reconeguda internacionalment.

E. Declaració d'aplicabilitat definitiva. Desenvolupament de la Declaració d'Aplicabilitat definitiva considerant el resultat de l'anàlisi de riscos. Aquest document s'haurà de mantenir actualitzat amb els canvis o controls que s'apliquin, de manera que sigui un eina útil per conèixer l'estat actual i el full de ruta pendent.

F. Política de seguretat. Definició, aprovació i publicació de la política de seguretat, recollint els objectius i missió de l'organització, els rols i responsabilitats, l'estructuració de comitès relacionats amb la seguretat i les directrius de gestió de la documentació.

3. PRESTACIÓ 173. SERVEI DE FORMACIÓ EN CIBERSEGURETAT.

3.1 SERVEI DE FORMACIÓ GENERAL EN CIBERSEGURETAT

El nostre servei de formació general està dissenyat per sensibilitzar el conjunt del personal de l'entitat contractant sobre els riscos associats a l'ús quotidià de les tecnologies digitals i proporcionar-los els coneixements bàsics per actuar de forma segura en el seu entorn laboral. Aquest servei és fonamental per reduir el vector d'amenaça humà i complementar les mesures tècniques amb una cultura de seguretat activa i transversal.

Les accions formatives es desenvolupen amb una orientació pràctica, clara i adaptada al nivell de coneixements dels participants, utilitzant metodologies participatives i exemples reals adaptats al sector públic local.

Objectius principals de la formació:

- Capacitar els empleats públics per identificar i evitar situacions de risc digital.
- Promoure bones pràctiques d'higiene digital, ús responsable de dispositius i protecció de dades.
- Incrementar el grau de conscienciació col·lectiva per prevenir incidents de ciberseguretat.

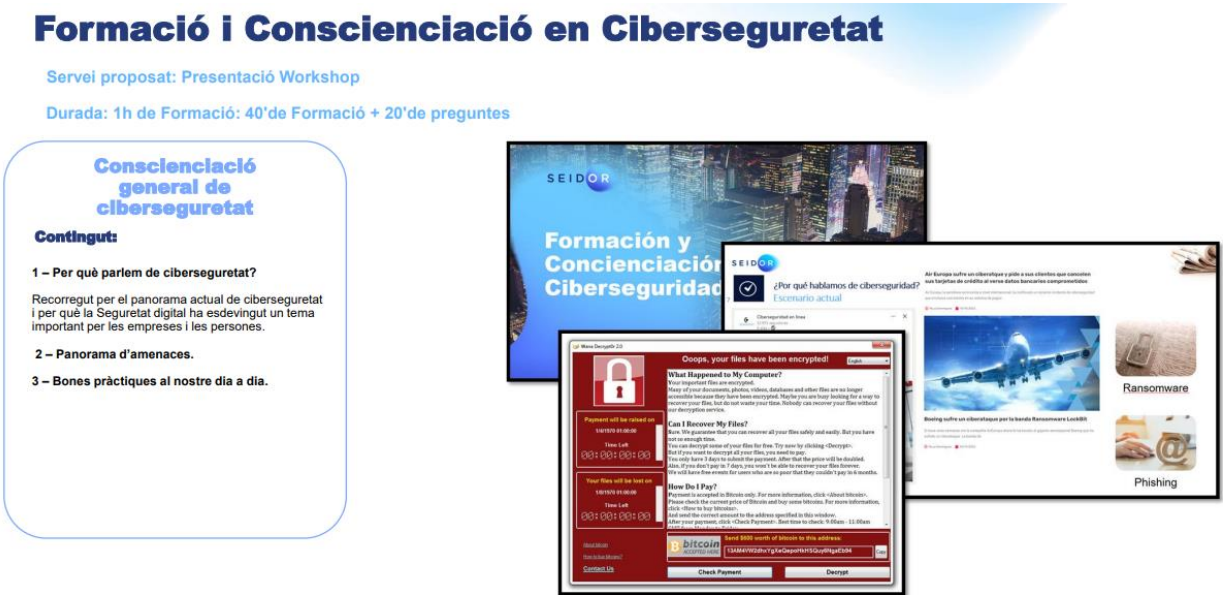
Metodologia i format:

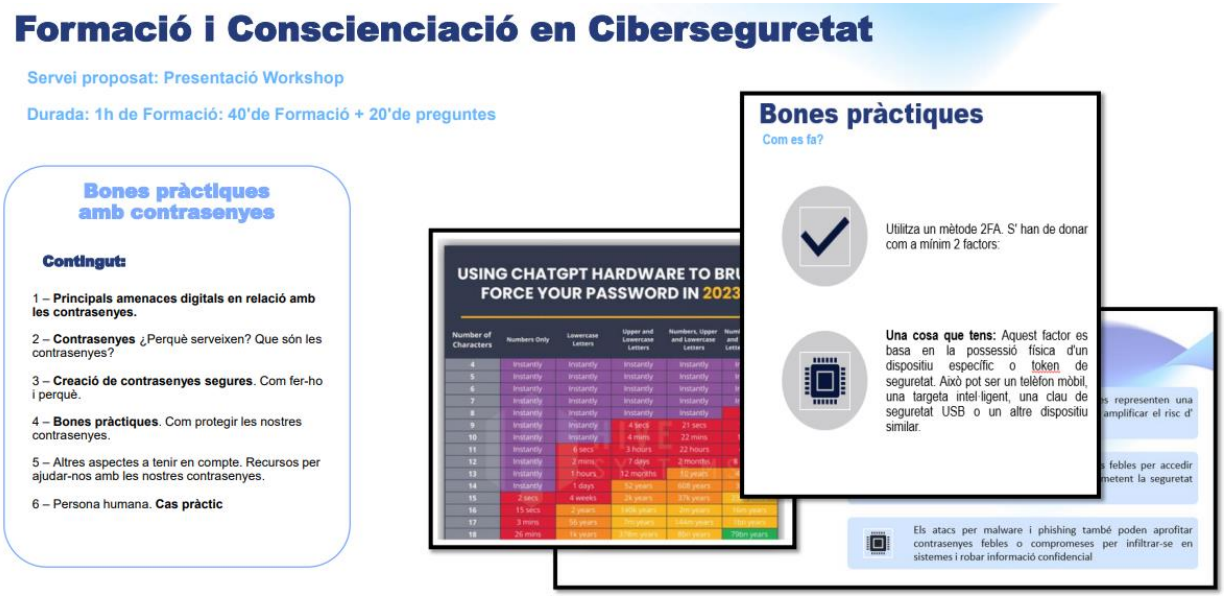
- Sessions tècniques intensives de 2 a 6 hores, presencials o remotes, segons l'entitat i els requisits concrets establerts als basats.
- Materials adaptats a les casuístiques de l'administració local i exemples reals.
- Possibilitat d'incloure mòduls optatius sobre tecnologies específiques (EDR, SIEM, MFA, etc.).
- Formadors certificats en ciberseguretat, amb experiència pràctica en implantació del ENS i en la realització de projectes de ciberseguretat.

Continguts:

Els continguts es podran presentar en diferents formats, principalment en forma de píndoles curtes o en presentacions detallades. Tots els formats inclouen una part de teoria sobre la matèria en qüestió, mes exemples i casos reals (a ser possible de proximitat), per tal d'impactar mes sobre els assistents.

A continuació, es mostren uns exemples il·lustratius de formacions disponibles. El catàleg complet contempla mes de 20 mòduls (amb formats mes curts o mes extensos) sobre temàtiques relacionades amb la ciberseguretat, i amb possibilitat de crear-ne de noves.





3.2 FORMACIÓ ESPECIALITZADA PER A RESPONSABLES TIC

La formació especialitzada que proposem està dirigida específicament a perfils tècnics, responsables TIC i personal amb rols clau en la gestió, implantació o supervisió de sistemes d'informació. L'objectiu és dotar aquest col·lectiu de les competències necessàries per desplegar i mantenir infraestructures segures, actuar davant incidents de ciberseguretat i assegurar el compliment normatiu vigent.

Aquest servei formatiu complementa la Prestació 172 d'assessorament tècnic i facilita l'apropiació efectiva del Sistema de Gestió de la Seguretat de la Informació (SGSI) que exigeix l'Esquema Nacional de Seguretat (ENS).

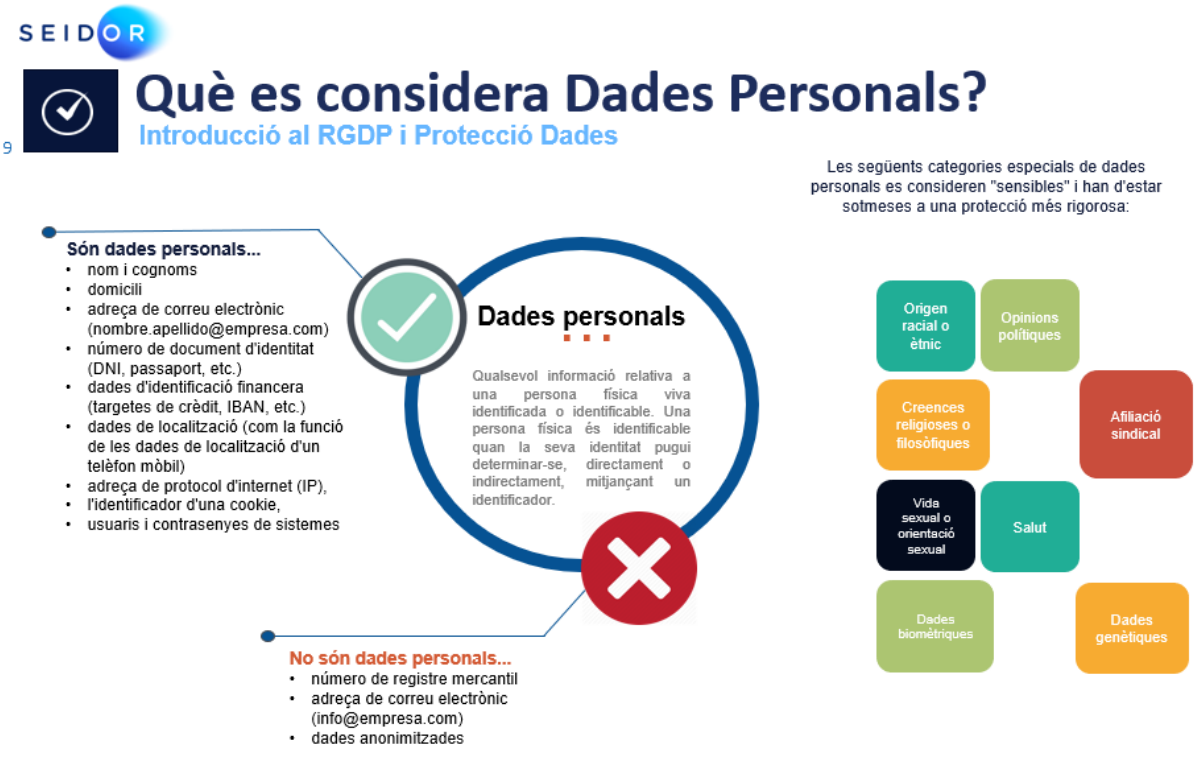
Objectius principals de la formació:

- Aprofundir en els requisits tècnics i organitzatius de l'ENS i altres normatives relacionades (RGPD, NIS2, etc.).
- Capacitar els responsables TIC en l'aplicació pràctica de controls de seguretat.
- Millorar la capacitat de resposta tècnica davant incidents i ciberamenaces avançades.
- Fomentar una cultura de governança de la seguretat a nivell operatiu.

Metodologia i format:

- Sessions tècniques amb component pràctic de 2 a 6 hores, presencials o remotes, segons l'entitat i els requisits concrets establerts als basats.
- Materials adaptats a les casuístiques de l'administració local i exemples reals.
- Possibilitat d'incloure mòduls optatius sobre tecnologies específiques (EDR, SIEM, MFA, etc.).
- Formadors certificats en ciberseguretat, amb experiència pràctica en implantació i administració de tecnologies de ciberseguretat.

Alguns exemples de continguts, en aquest cas sobre Protecció de dades:



4. COORDINACIÓ AMB L'ENTITAT LOCAL

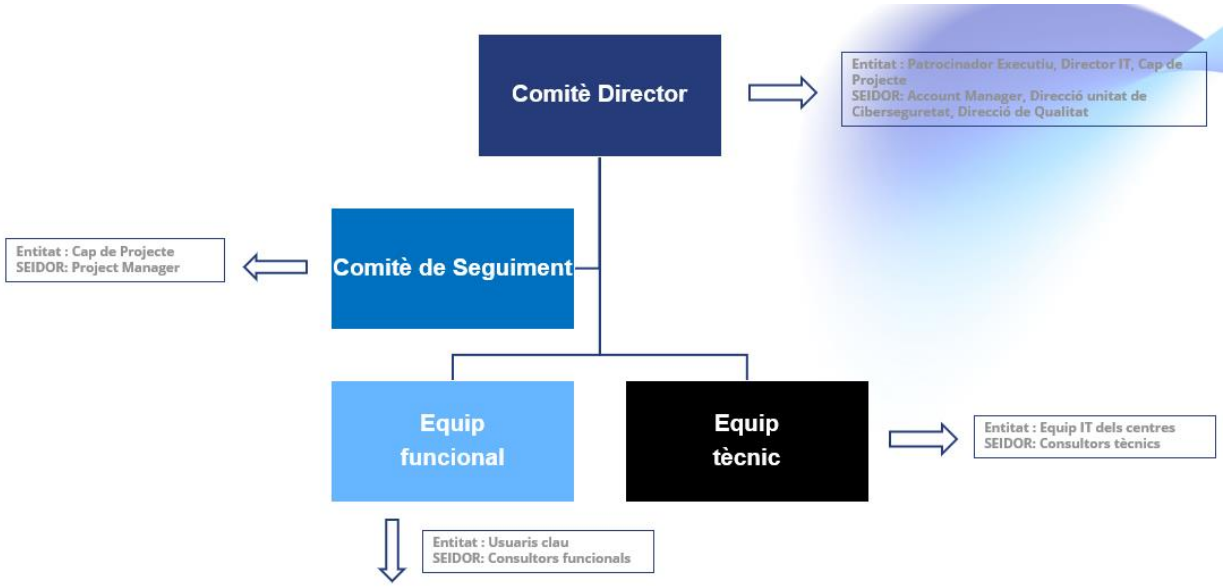
Una de les claus per a l'èxit de la prestació del servei és establir un model de coordinació estable, estructurat i bidireccional amb les entitats locals contractants. La nostra proposta s'articula al voltant d'una governança clara, canals de comunicació operatius i procediments ben definits per a la gestió d'incidències i la resposta davant situacions crítiques.

El projecte es desplega mitjançant una estructura tripartida de comitès (Direcció, Seguiment i Operatiu), que garanteix una interlocució fluida, traçabilitat de decisions i alineament estratègic i tècnic.

La comunicació es realitza per correu electrònic, telèfon i plataforma col·laborativa (Microsoft Teams o semblant), amb accés per als responsables designats per l'entitat. Aquesta plataforma permet:

- Seguiment centralitzat de tasques.
- Intercanvi de documentació.
- Registre d'incidències i consultes.
- Historial de comunicacions amb traçabilitat.

A més, s'ofereix la possibilitat d'establir una bústia única de suport per a la gestió de l'estat de les accions pendents, incidències i decisions.



Comitè Director:

- Participants: Direcció del client (patrocinador executiu, direcció TIC) i direcció de projecte per part del nostre equip.
- Funcions:
    - Presa de decisions estratègiques.
    - Validació d'evolució i compliment dels objectius.
    - Aprovació de canvis de servei, assignació de recursos i resolució de bloquejos.
    - Garantir l'alineament del servei amb les prioritats institucionals.

Comitè de Seguiment:

- Participants: Caps de projecte de cada part, amb rol de Service Manager per part de l'equip consultor.

- Funcions:
  - Planificació de tasques, revisió de fites i calendaris.
  - Seguiment de resultats, desviacions i riscos operatius.
  - Interlocució directa amb el client durant tota la prestació.
  - Supervisió contínua del desplegament del ENS o altres accions previstes.

Comitè Operatiu (Equip funcional i tècnic)

- Participants:
  - Per part del client: personal TIC i usuaris clau.
  - Per part de l'equip consultor: especialistes tècnics i funcionals en ciberseguretat.
- Funcions:
  - Execució de tasques d'implantació, revisió documental i manteniment de l'ENS.
  - Gestió del dia a dia del projecte, formació i accions de conscienciació.
  - Elaboració d'informes i actualització de registres de conformitat.

5. ASPECTES CLAUS EN MATÈRIA DE CIBERSEGURETAT

La seguretat de la informació constitueix un pilar essencial per al bon funcionament de qualsevol entitat pública, especialment en un context en què l'administració electrònica, la protecció de dades i els serveis digitals a la ciutadania depenen cada vegada més de la disponibilitat, integritat i confidencialitat dels sistemes d'informació. L'adequació al Esquema Nacional de Seguretat (ENS) i a la directiva NIS2 implica establir mecanismes robustos i proactius per protegir els actius crítics i garantir la continuïtat operativa davant qualsevol eventualitat.

Aspectes clau en matèria de seguretat de la informació:

Els principis rectors de la nostra actuació en matèria de seguretat de la informació es basen en:

- Gestió del risc continuada: identificació, anàlisi i tractament dels riscos en sistemes, processos i serveis crítics, mitjançant metodologies reconegudes (ex: MAGERIT, ISO/IEC 27005).
- Implementació de controls de seguretat: desplegament progressiu de mesures del Annex II del ENS, com la segmentació de xarxes, l'autenticació reforçada, el xifrat de dades i la monitorització dels sistemes.
- Governança de la seguretat: definició de rols i responsabilitats, creació de comitès de seguretat i establiment d'una política formal aprovada per direcció.
- Capacitació i sensibilització: formació del personal (tant tècnic com general) per garantir el seu alineament amb les bones pràctiques i les obligacions normatives.
- Registre i traçabilitat: ús de sistemes de logs, alertes i auditories internes per mantenir un seguiment efectiu i preventiu del comportament dels sistemes.

Aquest enfocament permet complir amb els cinc principis del ENS: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

Procediment d'actuació davant de desastres:

En cas d'incident greu o desastre (com ara un atac de ransomware, una pèrdua massiva de dades o una interrupció de serveis essencials), el procediment general proposat es basa en un model estructurat de resposta i recuperació. Òbviament, aquest procediment es generalista i

resumit i s'haurà de detallar perfectament per cada cas, part important de la implementació efectiva del ENS o NIS2.

1. Detecció i notificació immediata
    - Els sistemes de monitorització o el personal detecten l'incident.
    - Comunicació immediata al responsable de seguretat i activació del protocol de resposta.
2. Activació del pla de resposta a incidents
    - Aplicació de mesures de contenció per minimitzar l'impacte (aïllament de sistemes, tall de connexions compromeses).
    - Recollida d'evidències digitals per a l'anàlisi forense, seguint cadenes de custòdia establertes.
3. Anàlisi i erradicació
    - Avaluació tècnica de la causa i identificació del vector d'entrada.
    - Eliminació del codi maliciós o del component afectat.
    - Revisió dels controls compromesos i actualització immediata.
4. Recuperació i restauració
    - Restauració de sistemes afectats mitjançant còpies de seguretat validades.
    - Comprovació d'integritat post-restauració i reinici progressiu dels serveis.
5. Comunicació i notificació externa (si escau)
    - Informació a l'Agència de Protecció de Dades o Agència de Ciberseguretat de Catalunya, segons el tipus d'incident.
    - Comunicació interna a usuaris i grups afectats.
6. Anàlisi post-incident i pla de millora
    - Elaboració d'un informe complet amb lliçons apreses i accions de millora.
    - Reforç dels controls vulnerats i actualització del Pla de Continuïtat.

Aquest procediment s'integra dins del marc establert pel ENS i està alineat amb l'objectiu de garantir la resiliència operativa de l'entitat, tal com exigeix també la directiva NIS2.