Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

Expedient de contractació núm. 2024.01
Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya

Memòria tècnica **Sobre B**

PROPOSICIÓ TÈCNICA

El/la senyor/a Albert Casadejust Cristina com Administrador Únic, de l'empresa Omega Peripherals S.L., sota la seva responsabilitat, com a licitador/a de l'Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya (Exp. núm. 2024.01), declara que la proposta que presenta per el Lot 16 , compleix els requisits obligatoris del Plec de Prescripcions Tècniques (PPT) i normativa legal vigent

Recordem que:

Les empreses hauran d'aportar la següent documentació:

- ***Memòria** relativa als criteris subjectes a un judici de valor*

I, perquè consti, signa aquesta declaració responsable.

(Barcelona, 28 de Maig de 2025)

35093681M
ALBERT
CASADEJUST
(R: B60343076)

Firmado digitalmente por 35093681M ALBERT CASADEJUST (R: B60343076)
Fecha: 2025.05.29 10:56:32 +02'00'

El otro lado de la tecnología

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGULENL'ACORD MARC DEL SUBMINISTRAMENT DESOLUCIONS I SERVEIS GESTIONATS DE SEGURETAT TIC

Expedient nº:2024.01

28 de mayo de 2025

Proposta Tècnica l'Acord marc de subministrament d'equips informàtics i de serveis associats

ÍNDICE

1. COORDINACIÓ DEL SERVEI

1.1. Introducció

OMEGA PERIPHERALS basa la prestació del seu servei TIC en les millors pràctiques propugnades per ITIL. Per a portar a la pràctica aquesta metodologia d'una manera satisfactòria, Omega Peripherals es recolza en l'èxit d'implementacions anteriors en diversos clients utilitzant models provats i alineats amb les recomanacions i millors pràctiques, a més de comptar amb el suport d'un equip humà amb les capacitats adequades per a garantir la prestació del Servei i de les eines de gestió adequades.

L'objectiu és assegurar que els serveis s'ofereixin de manera efectiva i eficient, això inclou complir amb els requeriments del client, resoldre fallades en el servei, solucionar problemes i dur a terme operacions rutinàries.

El workflow que els presentem haurà d'integrar-se al model operatiu definit per l'entitat local i a les eines de l'entitat local si aquesta les té.

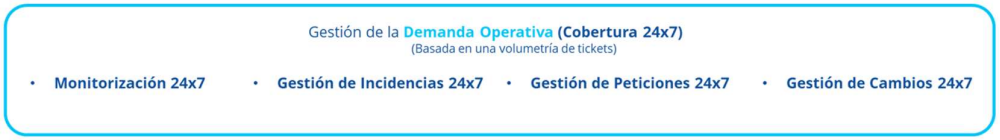
En la nostra oferta s'inclouen totes les funcions requerides per a garantir els nivells de servei exigits i de manera addicional, aquelles tasques de valor afegit que permetin una evident millora de les qualitats del servei dels sistemes en termes de reducció de costos, increment de rendiment, assegurament de qualitat i evolució tecnològica.

A continuació, es llisten algunes de les activitats habituals del servei:

- Coadministración i gestió de plataformes.
- Orientar el servei a assegurar la Continuïtat de negoci
- Gestió de la Configuració, documentació i coneixement de les plataformes, incloent-hi Control de versions i pegats.
- Modificacions i adequacions de la configuració de les plataformes.
- Generació de documentació operativa i de gestió de les plataformes per a nivells 1 i 2.
- Adquisició de coneixement en les eines i plataformes a operar.
- Cerca contínua de l'eficiència de processos operatius amb ajuda d'automatització i eines.
- Col·laboració amb fabricant per a solucionar problemes i anticipar-se als riscos.

1.2. Demanda Operativa

La demanda operativa són el conjunt de tasques encaminades a l'atenció i resolució d'Incidències, problemes i peticions operacionals sobre la plataforma. Aquesta demanda serà atesa tant pels equips de Nivell 1, Nivell 2 i Nivell 3 d'Omega Peripherals en 24x7. En funció del tipus d'Incidència, problema o petició i la seva SLA.



- Definir quins elements monitorar per a la correcta detecció d'esdeveniments/incidències. Ajust fi dels nivells de tolerància.

- Assegurar que els diferents components que donen servei a les plataformes estiguin correctament monitorats.
- Identificar i categoritzar els esdeveniments que es produeixin en les plataformes.
- Recepció i resolució d'incidències associades a les plataformes.
- Obertura, seguiment i resolució d'incidències amb fabricant. Publicació en *KB de "*work *around" a seguir per a incidències identificades com a repetitives.
- Gestió de Problemes de les plataformes. Categorització dels problemes. Resolució dels problemes que apareguin en l'àmbit de les plataformes.
- Prevenir incidents i minimitzar l'impacte d'aquells Incidents que no poden prevenir-se
- Manteniment del catàleg de serveis.

1.2.1. Gestió de la demanda Operativa

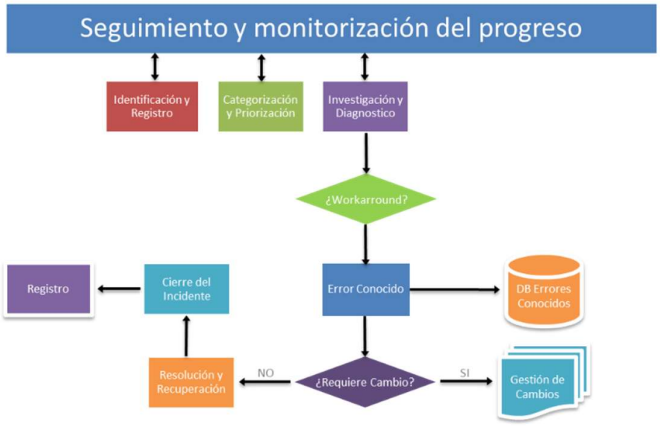
La demanda operativa són el conjunt de tasques encaminades a l'atenció i resolució d'Incidències, problemes i peticions operacionals sobre la plataforma. Aquesta demanda serà atesa tant per l'equip d'Omega Peripherals. En funció del tipus d'Incidència, problema o petició i la seva SLA aquesta serà atesa per un equip o un altre, podent escalar la incidència entre equips.

La volumetria associada a aquesta demanda serà mesurada pel nombre de tiquets i serà gestionat per l'eina de Ticketing d'Omega Peripherals o de l'entitat local, segons es defineixi en l'alta del servei.

1.2.2. Gestió d'Incidències

Per a garantir la resposta del servei en el 100% dels casos, dins de l'horari del servei es dedicarà un equip de tècnics en infraestructures TU amb el grau de coneixement necessari per a identificar i classificar la incidència adequadament atesos els nivells de severitat definits i consensuats amb el client, escalant la incidència a nivells superiors o als fabricants si calgués i realitzant totes les accions que siguin necessàries per a la seva resolució en el menor temps possible.

La metodologia que se segueix quant a la gestió d'Incidències es descriu en el següent esquema:



Es contemplen les següents activitats dins d'aquest servei:

- Recepció, Identificació i registre d'incidències
- Categorització i priorització de la incidència, problema o avaria en funció de la seva criticitat i impacte.
- Proporcionar solucions temporals (workarounds) i pegats per a pal·liar l'impacte.

- Recerca i diagnòstic.
- Escalat al suport especialitzat (suporti 3r nivell i fabricants)
- Control i seguiment de l'estat de la incidència,
- Registre de tota la documentació tècnica elaborada durant la incidència
- Proposar RFCs (Request for Changes) per a dur a terme la implementació de les solucions als problemes
- Tancament de les incidències
- Analitzar i determinar les causes d'Incidents recurrents i proposar solucions
- Realitzar seguiments dels orígens i solucions als problemes
- Estudiar tendències per a prevenir Incidents potencials
- Recol·lecció d'informació sobre els problemes

Quan les Incidències es resolen, la informació sobre la resolució queda registrada el que permet accelerar el temps de resolució i determinar futures solucions sobre la base de les existents, reduint el temps de resolució d'Incidències. Gràcies a això s'aconsegueix un menor temps d'inactivitat i interrupció en els sistemes més crítics de negoci.

1.2.3. Gestió de Peticions

Dins de l'horari del servei es dedicarà un equip de tècnics en infraestructures TU amb el grau de coneixement necessari per a identificar i classificar la petició, atesos els nivells de severitat definits i consensuats amb l'entitat local realitzant totes les accions que siguin necessàries per a la seva implementació en el menor temps possible.

La metodologia que se segueix quant a la gestió d'Incidències es descriu en el següent esquema:

Es contemplen les següents activitats dins de la Gestió de Peticions:

- Recepció i registre de Peticions
- Categorització i priorització de la petició
- Registre de tota la documentació tècnica elaborada durant la petició
- Actualitzar la informació en Gestió de Canvis.
- Tancament de la petició

1.2.4. Gestió de Canvis

Dins de l'horari del servei l'equip tècnic d'infraestructures TU seran també els responsables de la gestió de canvis.

Es contemplen les següents activitats dins d'aquesta Gestió:

- Recepció i registre del canvi
- Preparació del *RFC del canvi.
- Gestionar el cicle d'aprovacions
- Planificar el canvi
- Obrir, executar i tancar el canvi dins del termini i en la forma escaient.

1.2. SLA del servei

D'acord amb l'indicat en el plec els serveis tindran un acord de nivell de servei com indica la següent taula com a mitja i descripció:

- Alta: incidències que suposen una aturada dels sistemes d'informació de l'entitat o que generen un impacte reputacional significatiu.
- Mitjana: incidències que afecten al funcionament de més d'un 5% dels empleats de l'entitat.
- Baixa: incidències que generen un funcionament incorrecte, però permet continuar treballant als empleats de l'entitat

Nivell de criticitat	Temps de resposta	Temps de resolució
Alta	60 min	4 hores
Mitjana	4 hores	48 hores
Baixa	48 hores	5 dies

1.3. Gestió d'amenaces i alertes

Es prioritzen amenaces mitjançant anàlisi contextual i classificació per nivells. Les alertes es canalitzen mitjançant SIEM i SOCs. S'activen respostes automàtiques o manuals amb recol·lecció d'evidències conforme a cadena de custòdia.

Marc general d'actuació

La gestió d'amenaces i alertes s'estructura sobre la base d'un model de cicle continu de millora, que integra les següents fases:

- Detecció
- Classificació i priorització
- Notificació i comunicació
- Contenció i mitigació
- Recol·lecció d'evidències
- Avaluació post incident

Aquest model és compatible amb els principals marcs de referència com a ISO/IEC 27035 (gestió d'incidents de seguretat) i NIST SP 800-61 (Computer Security Incident Handling Guide), assegurant una resposta estructurada i alineada amb les millors pràctiques internacionals.

Sistema de detecció i correlació d'esdeveniments (SIEM)

Proposem com a base tecnològica l'ús d'una solució de SIEM (Security Information and Event Management) com a centre neuràlgic de la detecció d'amenaces. Aquesta plataforma permetrà:

- Agregar, normalitzar i analitzar esdeveniments de múltiples fonts (firewalls, antivirus, servidors, xarxes, endpoints, etc.)
- Aplicar regles de correlació per a identificar patrons anòmals o sospitosos
- Generar alertes automàtiques en funció dels indicadors de compromís (IoC)
- Integrar fonts d'intel·ligència d'amenaces (Threat Intelligence)

La solució SIEM proposta podrà ser de tipus open-source (com Wazuh o TheHive+Cortex) o comercial (com Splunk o IBM QRadar), adaptant-se a les característiques i pressupost del client. Comptarà amb capacitat d'integració amb eines EDR, NDR i sistemes SCADA si aplica.

Priorització i classificació d'amenaces

Una vegada generada una alerta per part del sistema SIEM o una altra font (usuari, sistema IDS, auditoria), s'activa el procés de classificació i priorització. Per a això, es defineixen criteris objectius:

- Gravetat de l'incident: segons afectació a la confidencialitat, integritat o disponibilitat
- Impacte potencial: usuaris afectats, serveis compromesos, pèrdua de dades, reputació
- Probabilitat d'ocurrència
- Nivell de criticitat del sistema afectat
- Naturalesa de l'amenaça: malware, ransomware, accés no autoritzat, fuga d'informació, etc.

Aquests criteris són avaluats automàticament per l'eina SIEM mitjançant regles predefinides i, si és necessari, validats per l'equip d'analistes.

S'empra una matriu de risc que classifica els incidents en nivells (alt, mitjà, baix) i en funció d'això es defineix el SLA de resposta i escalat

Notificació i comunicació d'incidents

Un dels principis clau d'una bona gestió és la comunicació eficaç i oportuna d'incidents. La nostra solució contempla:

- Notificacions automàtiques a través de correu electrònic, missatgeria segura o dashboard
- Activació de protocols de comunicació interna i externa (equips IT, responsables de seguretat, autoritats competents)
- Generació automàtica de reportis preliminars i finals
- Comunicació amb el Centre Criptològic Nacional (CCN-CERT) quan escaigui, conforme als requisits del ENS

A més, es proporcionaran canals segurs per a la recepció de denúncies o avisos d'usuaris o tercers, garantint la traçabilitat i la gestió adequada de cada cas.

Mesures de contenció

La contenció immediata d'una amenaça és fonamental per a minimitzar l'impacte. Depenent del tipus d'incident i de l'entorn afectat, s'aplicaran mesures com:

- Aïllament de dispositius afectats
- Cort de comunicacions de xarxa
- Desactivació temporal de comptes o serveis
- Aplicació de regles en firewalls i sistemes EDR
- Contenció lògica en sistemes virtualizados o contenidors
- Pegats urgents de vulnerabilitats explotades

Aquestes accions estan protocol·litzades i seran executades segons els Playbooks definits per a cada tipologia d'amenaça. Aquests playbooks estan prèviament validats amb el client i permeten una actuació àgil i consensuada.

Sistemes de resposta automatitzada

Amb la finalitat de reduir el temps de resposta i la càrrega operativa, proposem integrar sistemes de resposta automatitzada (SOAR – Security Orchestration, Automation and Response), que permeten:

- Automatitzar tasques repetitives com el bloqueig de IPs, anàlisi de malware, quarantena de hosts
- Executar fluxos predefinits de resposta segons el tipus d'alerta
- Escalar automàticament a responsables quan l'incident el requereix

El sistema SOAR pot integrar-se amb el SIEM i altres eines existents del client, assegurant una resposta coherent i traçable.

Recol·lecció i custòdia d'evidències

Tota actuació en matèria de ciberseguretat ha d'estar recolzada per una adequada recol·lecció d'evidències digitals, tant per a la seva anàlisi forense com per al seu possible ús jurídic. Per a això:

- S'estableixen procediments normalitzats de captura de logs, imatges de disc, dumps de memòria i altres artefactes digitals
- S'aplica la cadena de custòdia, documentant cada acció realitzada sobre les evidències
- Les evidències s'emmagatzemen en repositoris segurs, xifratges i amb accés restringit
- S'empren eines forenses especialitzades (Autopsy, Volatility, FTK Imager)

A més, si el client el requereix, es facilitarà un informe forense pericial elaborat per personal qualificat i amb validesa legal.

Eines complementàries proposades

Per a reforçar la gestió integral d'alertes i amenaces, proposem l'ús de:

- Wazuh: com a sistema SIEM/IDS open-source
- TheHive + Cortex: per a la gestió col·laborativa d'incidents
- MISP (Malware Information Sharing Platform): per a compartir i enriquir intel·ligència d'amenaces
- GRR Rapid Response o Velociraptor: per a resposta en endpoints a nivell forense
- Suricata / Zeek: per a inspecció de trànsit en xarxa

Aquestes eines permeten una cobertura completa del cicle de vida de l'incident, des de la detecció fins a l'anàlisi post mortem.

Capacitació i sensibilització

La tecnologia no és suficient si no està acompanyada d'una formació adequada del personal. En aquest sentit:

- S'impartiran formacions periòdiques per als equips IT i responsables de seguretat
- Es realitzaran simulacres d'incidents reals (Exercicis Tabletop i Xarxa Team)
- Es desenvoluparan manuals operatius i protocols adaptats a l'entorn del client
- S'establirà un sistema de lliçons apreses per a millorar contínuament

A més, es fomentarà la cultura de ciberseguretat entre els usuaris finals perquè actuïn com a sensors addicionals davant incidents.

Informes i KPIs

Tota actuació serà objecte de registre i seguiment mitjançant informes periòdics que incloguin:

- Estadístiques d'incidents detectats, classificats per tipus, criticitat i origen
- Temps de resposta i resolució (SLA compliments)
- Accions de contenció i recuperació realitzades
- Evolució temporal i comparatives històriques
- Lliçons apreses i mesures de millora

Es definiran indicadors clau (KPIs) per a avaluar l'acompliment del servei, com:

- Temps mitjà de detecció (MTTD)
- Temps mitjà de resposta (MTTR)
- Percentatge d'incidents continguts sense afectació crítica
- Compliment de notificacions a CCN-CERT

Coordinació amb el client i tercers

En cas que el client compti amb altres proveïdors o amb personal intern que gestioni part de la infraestructura, s'establiran canals de coordinació clars i eficients, que assegurin:

- Flux constant d'informació i retroalimentació
- Definició de responsables en cada fase de l'incident
- Priorització d'actuacions segons impacte i responsabilitat
- Gestió de conflictes i presa de decisions ràpida

També es preveu la col·laboració amb equips nacionals de resposta (INCIBE, CCN-CERT) o forces de seguretat, quan la gravetat de l'incident el requereixi.

Integració amb altres serveis del lot

La gestió d'amenaces i alertes està plenament alineada amb altres components del Lot, com:

- Monitoratge proactiu
- Gestió de vulnerabilitats
- Gestió d'identitats i accessos
- Anàlisis de riscos i compliment del ENS

Aquesta visió holística permet actuar de forma anticipada i coordinada, minimitzant l'exposició a amenaces i assegurant la resiliència operativa.

1.4. Resposta a incidents

Capacitat de detecció, anàlisi i remediació immediata. Recerca detallada i generació d'informes per incident. Coordinació amb responsables de l'organisme i serveis CERT. S'apliquen plans de contenció i s'analitza l'impacte amb proposta de millores.

Organització operativa per a la resposta

Equips implicats

Per a assegurar una resposta eficaç davant qualsevol tipus d'incident, es constituirà un Equip de Resposta davant Incidents de Seguretat Informàtica (CSIRT). L' equip estarà format pels diferents perfils professionals:

- Responsable del Servei / CISO, analistes de primer nivell (Tier 1), analistes de segon nivell, experts en contenció i recuperació, comunicacions i relació institucional.

Cadascun d'aquests perfils compta amb formació certificada (CISSP, CISM, CEH, OSCP, CRISC, etc.) i experiència demostrada en entorns de ciberseguretat crítics, especialment en el sector públic.

Procés de resposta a incidents

El procés d'actuació s'estructura en sis fases, conforme a les millors pràctiques internacionals:

1. Preparació

Aquesta fase consisteix a establir polítiques, procediments, eines i competències necessàries per a una resposta efectiva. Inclou:

- Desenvolupament i validació del Pla de Resposta a Incidents (PRI).
- Assignació de rols i responsabilitats clares.
- Disponibilitat d'eines SIEM, EDR, SOAR i forenses.
- Simulacres periòdics (Exercicis Tabletop).
- Inventariat actualitzat d'actius i topologies.

2. Detecció i anàlisi

Qualsevol esdeveniment anòmal detectat per sistemes automàtics (SIEM, EDR, IDS, etc.) o reportat per usuaris és avaluat immediatament. L'anàlisi inclou:

- Classificació de l'incident (malware, accés no autoritzat, denegació de servei, fuga d'informació…).
- Determinació de l'abast i sistemes afectats.
- Correlació amb esdeveniments anteriors o campanyes conegudes.
- Extracció de IoCs i TTPs de l'atacant (segons MITRE ATT&CK).
- Valoració de la severitat i criticitat.

3. Contenció

Una vegada confirmat l'incident, s'activen mesures per a detenir la seva propagació. Existeixen tres nivells:

- Contenció immediata: aïllament de endpoints, bloqueig de trànsit sospitós.
- Contenció a curt termini: canvis de contrasenyes, ajustos en polítiques, filtrat en servidors.
- Contenció a llarg termini: revisió de configuracions, desactivació d'accessos innecessaris, aplicació de pegats.

Les accions són acuradament registrades per a mantenir la cadena de custòdia.

4. Erradicació

L'objectiu és eliminar completament l'amenaça de l'entorn. Inclou:

- Identificació de vectors d'entrada i vulnerabilitats explotades.
- Eliminació de malware, backdoors o comptes compromesos.
- Reinstal·lació de sistemes des d'imatges segures.
- Revisió exhaustiva de logs per a confirmar la neteja.

Aquesta fase és crítica per a evitar reinfeccions o persistències indesitjades.

5. Recuperació

Es treballa per a restaurar la funcionalitat completa i normal dels sistemes:

- Restauració de còpies de seguretat.
- Reintegració d'equips aïllats.
- Monitoratge reforçat post-incident.
- Validació de la integritat operativa.

El temps de recuperació s'ajusta segons l'impacte i la criticitat de l'incident.

6. Lliçons apreses i millora contínua

Finalitzat l'incident, es realitza un informe detallat que inclou:

- Cronologia completa de l'esdeveniment.
- Accions realitzades per cada actor.
- Anàlisi de causa arrel (RCA).
- Recomanacions per a evitar recurrències.
- Revisió i actualització de procediments.

Aquest informe es comparteix amb l'entitat i, si escau, amb autoritats competents.

Coordinació amb agents interns i externs

Internament

S'estableixen protocols de comunicació estructurats per als diferents nivells de l'entitat:

- Àrea tècnica (IT)
- Adreça
- Usuaris finals
- Delegat de Protecció de Dades

S'empren eines de comunicació segures (correu xifrat, missatgeria protegida, canals privats).

Externament

En funció de la naturalesa de l'incident, s'activa la col·laboració amb:

- CCN-CERT: conforme als requisits del ENS.
- INCIBE-CERT: en cas d'afectació a serveis essencials.
- Forces i cossos de seguretat de l'Estat: si l'incident revesteix caràcter delictiu.
- Proveïdors tecnològics: per a suport específic (Microsoft, Cisco, etc.).
- ASSEGURADORES o entitats legals: en cas de reclamacions o bretxes de dades personals.

Es garanteix el compliment dels terminis i formats establerts per la legislació (per exemple, el RGPD exigeix comunicar bretxes de seguretat en un termini màxim de 72 hores).

Capacitats diferencials de resposta

La nostra proposta aporta un alt nivell de maduresa i capacitats destacades:

- Playbooks personalitzats per tipus d'incident.
- Integració amb plataformes de Threat Intelligence i MISP.
- Eines d'anàlisis forense (Volatility, FTK, Autopsy).
- Possibilitat d'intervenció en camp en menys de 4h (si aplica).
- Generació d'informes tècnic-legals i assessorament en compliment normatiu.
- Simulacions periòdiques per a validar l'eficàcia de la resposta.

Indicadors i seguiment del servei

Per a garantir la traçabilitat i qualitat del servei de resposta, es monitoren indicadors clau:

- Temps mitjà de detecció, contenció i resolució
- Nombre d'incidents crítics gestionats
- Incidents detectats vs. incidents reportats
- Resultats de simulacres i exercicis d'estrès

Aquests indicadors seran reportats a l'entitat de manera mensual o trimestral, juntament amb propostes de millora.

Adaptació a l'entitat pública local

Tots els procediments, eines i respostes seran ajustats de forma personalitzada a la realitat operativa de l'entitat. Per a això:

- Es realitzarà una fase inicial de coneixement i documentació.
- Es validaran els actius més crítics i els processos sensibles.
- S'adaptaran els playbooks i protocols de resposta a l'estructura i eines utilitzades per l'administració local.
- Es designarà un interlocutor tècnic que mantindrà contacte directe amb l'entitat per a totes les qüestions relacionades amb incidents.

1.5. Metodologia i enfocament didàctic

La formació es basa en els principis de l'aprenentatge actiu, pràctic i col·laboratiu. Les sessions combinen continguts teòrics amb activitats participatives, simulacions, resolució de casos reals i dinàmiques de grup.

S'adaptaran els continguts al nivell de coneixements dels participants, aplicant un enfocament de educació d'adults, personalitzat i orientat a resultats.

La modalitat d'impartició podrà ser:

- Presencial
- Virtual sincrònica
- Blended learning (combinada)

S'utilitzaran eines com Moodle per a seguiment de cursos en línia, videoconferències interactives (Zoom, Teams), materials descarregables i fòrums de debat.

1.7. Tipus de sessions.

Sessions breus de conscienciació (1,5 h)

Aquestes sessions combinen presentacions lleugeres, exemples reals, enquestes en directe i resolució de dubtes.

Avaluació de l'aprenentatge i certificació nivell bàsic

En els cursos avançats es podrà emetre certificat amb equivalència de crèdits formatius si l'entitat ho requereix.

Eines i recursos didàctics

Diverses solucions de simulació, qüestionaris , manuals i guies com a recurs.

Formació ad hoc

A més dels cursos detallats anteriorment, s'ofereix la possibilitat de dissenyar accions formatives totalment a mesura.

Aquest disseny inclou fases d'anàlisis de necessitats, validació de temaris i metodologia, impartició adaptada i avaluació d'impacte.

La metodologia proposada per al disseny, desenvolupament i execució de formació a mesura consta de cinc fases principals, amb activitats concretes en cadascuna