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

Annex núm. 03. LOTS 18 a 41 **Sobre B**

PROPOSICIÓ TÈCNICA

El senyor Guillem Treserra Prat, com a apoderat, de l'empresa **AIGÜES VIC ENGINYERIA I TECNOLOGIA S.L.**, amb NIF B10721355, sota la seva responsabilitat, com a licitador 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 els Lots 34, 35, 36, 37, 38, 39, 40 i 41 compleix els requisits obligatoris del Plec de Prescripcions Tècniques (PPT) i normativa legal vigent

Recordem que:

Les empreses hauran d'aportar aquest ***Annex núm. 03*** *degudament complimentat i acompanyat de la següent documentació:*

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

I, perquè consti, signa aquesta declaració responsable.

Vic, a data de la signatura electrònica

38115478Q GUILLEM TRESERRA (R: B10721355)

Firmado digitalmente por 38115478Q GUILLEM TRESERRA (R: B10721355)
Fecha: 2025.05.29 11:31:37 +02'00'

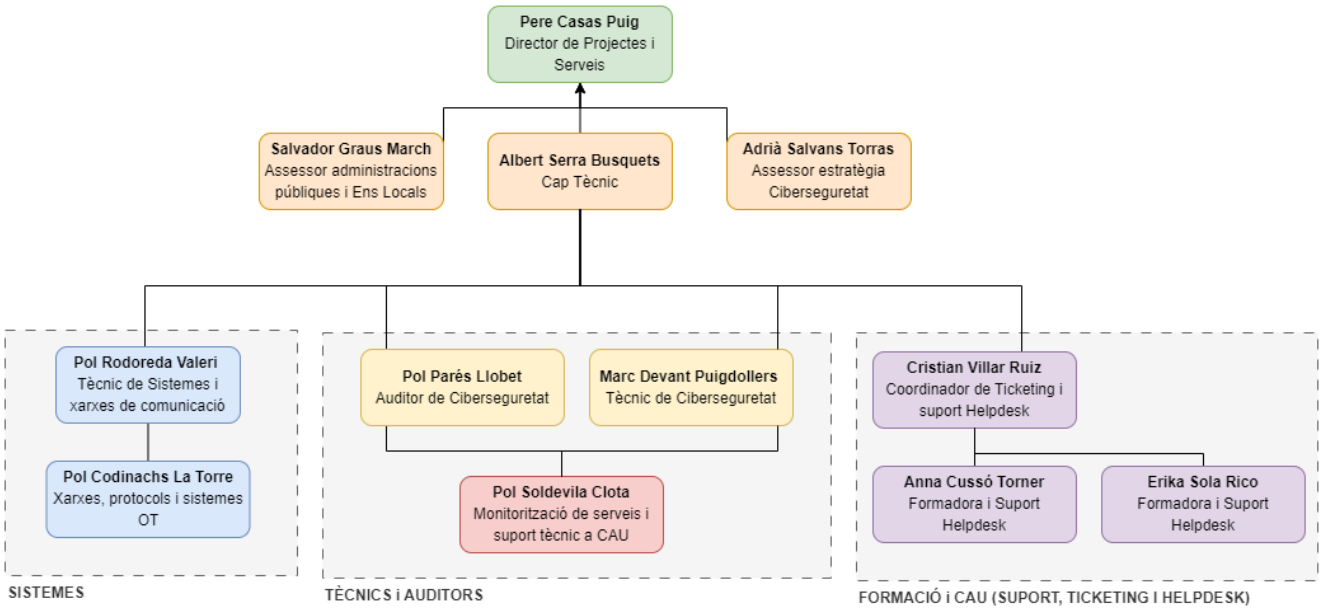
MEMÒRIA TÈCNICA: Proposta pels LOTS 34 a 41 de serveis de Ciberseguretat

ÍNDEX

1. Proposta d'organigrama tècnic adscrit al present acord marc

Aigües Vic Enginyeria i Tecnologia, SL, d'ara en endavant AVENTEC, és una empresa especialitzada en la prestació de serveis d'enginyeria, solucions digitals i serveis de ciberseguretat integrals, a les empreses i administracions que gestionen el cicle urbà de l'aigua, generalment sector públic, i sobretot ens locals. Actualment, els serveis que s'ofereixen des d'AVENTEC, i en concret els de ciberseguretat, ja s'estenen més enllà del sector de l'aigua, a la resta de sector municipal, sobretot, i també a empreses. Per tant, des d'AVENTEC, es disposa d'una sòlida experiència en la prestació de serveis de ciberseguretat als ens locals.

Des d'AVENTEC, es proposa la realització els serveis de ciberseguretat dels Lots 34 a 41 amb el següent equip tècnic:



Proposta d'organigrama tècnic adscrit al present acord marc

Aquest equip està composat pels tècnics necessaris per donar un servei complet als ens locals de Catalunya. Està composat per tècnics experts en ciberseguretat, rols de perfil d'atenció a l'usuari, formadors, tècnics de sistemes amb coneixement transversal a la tecnologia i perfils estratègics per enfocar d'una forma òptima els serveis i el tracte i processos amb els ens locals. Seguidament es detallen a la següent taula.

Personal	Rol	Funció
Pere Casas Puig	Director de Projectes i Serveis	Coordinació general de projectes, supervisió de l'execució dels serveis i gestió estratègica dels recursos.
Salvador Graus March	Assessor administracions públiques i ens locals	Suport i assessorament per la prestació de serveis i projectes a les administracions públiques i ens locals en matèria de ciberseguretat i altres serveis.
Albert Serra Busquets	Cap tècnic	Direcció tècnica dels serveis, definició d'estratègies de millora i supervisió de les activitats tècniques
Adrià Salvans Torras	Assessor estratègia Ciberseguretat	Definició de plans de millora i estratègies de ciberseguretat adaptades a cada organització.

Pol Parés Llobet	Auditor de Ciberseguretat	Execució d'auditories tècniques i de compliment, identificació de vulnerabilitats i propostes de millora.
Marc Devant Puigdollers	Tècnic de Ciberseguretat	Implementació de mesures de ciberseguretat i suport tècnic especialitzat en entorns crítics.
Pol Soldevila Clota	Monitorització de serveis i suport tècnic a CAU	Monitoratge continuat dels serveis i assistència tècnica al Centre d'Atenció a l'Usuari (CAU).
Cristian Villar Ruiz	Coordinador de Ticketing i suport Helpdesk	Coordinació i gestió eficient del suport Helpdesk, resolució d'incidències i atenció a les consultes.
Anna Cussó Torner	Formadora i Suport Helpdesk	Formació especialitzada en ciberseguretat i suport a l'usuari per a la resolució de dubtes.
Erika Sola Rico	Formadora i Suport Helpdesk	Formació pràctica en bones pràctiques de ciberseguretat i assistència personalitzada a l'usuari.
Pol Rodoreda Valeri	Tècnic de sistemes i xarxes de comunicació	Instal·lació, configuració i manteniment de sistemes i xarxes de comunicació amb enfocament segur.
Pol Codinachs La Torre	Tècnic de xarxes, protocols i sistemes OT	Implantació de mesures de ciberseguretat específiques en entorns OT i supervisió de protocols industrials.

Taula de personal, rols i funcions

2. Coordinació entre AVENTEC i l'ens Local

Aquest apartat té com a objectiu establir de manera clara com es durà a terme la coordinació entre AVENTEC i l'ens local per assegurar que els serveis de ciberseguretat es desenvolupin de forma fluida i efectiva.

En aquest punt s'identifiquen les dues parts involucrades:

- **AVENTEC**, que serà l'empresa responsable de desplegar els serveis de ciberseguretat i oferir el suport tècnic necessari. A l'apartat anterior es detalla els rols de l'equip a prestar el servei.
- **L'ens local**, que és el client que rebrà aquests serveis i participarà activament en la seva implementació i seguiment.

Els rols de cada membre de l'ens local implicat en els serveis són:

- **Responsable Tècnic de l'ens local**:
  És el contacte principal de referència. Aquest tècnic serà qui mantingui la coordinació contínua amb AVENTEC i tingui una visió general dels serveis a desplegar.
  🔑 *Funció clau: Coordinació principal i continua.*
- **Empresa de sistemes subcontractada**:
  Si l'ens local té una empresa de sistemes subcontractada, aquesta es podrà implicar opcionalment per ajudar en la implementació de les mesures i el manteniment.
  🔑 *Funció opcional: Suport a la implementació i manteniment.*
- **Tècnic informàtic adscrit del Consell Comarcal o tècnic informàtic de l'Ens**:
  En cas que existeixi, aquest tècnic pot complementar les tasques de coordinació i oferir un suport tècnic addicional.
  🔑 *Funció opcional: Suport a la implementació i manteniment, i donar suport a la coordinació.*
- **Personal tècnic, administratiu i polític de l'ens local**:
  Aquests són els usuaris finals o les persones a qui els serveis de ciberseguretat poden tenir

un impacte directe. És important tenir-los en compte en les fases de desplegament i adaptació dels serveis.

Funció: Públic objectiu dels serveis.

3. Canals de comunicació entre AVENTEC i l'Ens Local

Els canals de comunicació també són un aspecte clau per donar un bon servei de qualitat. Es defineixen els següents:

Canal de comunicació	Ús principal
Presencial	Reunions o sessions de treball amb atenció directa i detallada.
Correu electrònic	Comunicacions oficials, seguiment de temes i enviament de documentació.
Mòbil / telèfon	Consultes o coordinacions ràpides que requereixin resposta immediata.
WhatsApp	Comunicacions informals o notificacions, sempre que ambdues parts hi estiguin d'acord.
Plataforma de ticketing i seguiment	Gestió d'incidències i seguiment de sol·licituds de manera organitzada.
Videotrucada (Teams, Meet o Zoom)	Reunions telemàtiques, presentacions o coordinacions amb interacció directa a distància.

Taula de canals de comunicació

4. Protocol de gestió i resolució d'incidències

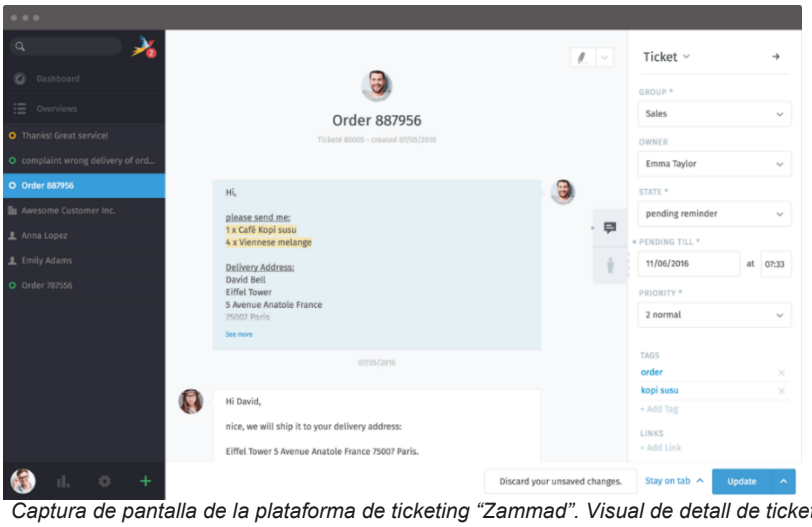
La gestió d'incidències cobreix l'atenció i resolució de qualsevol incidència, petició o consulta que afecti a la ciberseguretat de l'ens local. A continuació es descriu el protocol d'actuació, la classificació d'incidències, el SLA (Acord de Nivell de Servei) que s'aplica, els canals d'atenció, el procediment d'escalat i el mecanisme de mesurament.

4.1.1. Protocol d'atenció d'incidències

- Recepció: cada incidència registrada per l'ens local en l'eina de ticketing rep un identificador únic i una confirmació automàtica per correu.
- Classificació de incidències: l'equip de suport assigna la incidència a un nivell (Avaries molt greus, Avaries greus, Avaries lleus) segons impacte i urgència.
- Classificació de peticions: l'equip de suport assigna la incidència a un nivell de peticions urgents o peticions no urgents.
- Assignació i diagnòstic: el ticket es derivarà al perfil tècnic responsable (Tècnic de Ciberseguretat, Cap Tècnic, Tècnic de Sistemes…).
- Resolució: el tècnic documenta diagnòstic, solució i proves en el mateix ticket.
- Tancament: un cop validada la correcció, el ticket es tanca amb evidències (logs, captures) i notificació automàtica a l'ens local.
- Escalat: si no hi ha resposta dins el temps màxim definit, el sistema escala automàticament al Cap Tècnic i, si s'escau, al Director de Projecte.

4.1.2. Accés i interacció amb l'eina de ticketing

Des d'AVENTEC es proporciona una eina de ticketing amb les següents característiques.



Captura de pantalla de la plataforma de ticketing "Zammad". Visual de detall de ticket.

- L'ens local disposa d'usuaris i rols configurats amb accés self-service per obrir, comentar i tancar tickets.
- Visibilitat en temps real: dashboards amb estats dels tickets (nous, en curs, pendents de resposta, tancats) i filtres per nivell, mòdul i data.
- Comunicació bidireccional: l'ens local pot adjuntar documents, captures i comentaris; l'equip tècnic respon a través del mateix canal.
- Notificacions configurables: alertes per correu o push al portal sobre canvis d'estat, assignacions i venciments de SLA.
- Formació i suport: sessions inicials per als usuaris de l'ens local sobre l'ús del portal i manual d'usuari accessible en línia.

4.1.3. Mecanismes de compliment dels paràmetres SLA 24x7

AVENTEC garanteix els temps mínims de resposta i resolució per a cada categoria, tenint en compte 24hores i 7 dies a la setmana i festius inclosos, comptabilitzats automàticament en l'eina de ticketing:

Nivell	Temps màx. 1a resposta en hores	Temps màx. Resolució
Avaries molt greus	1 hores	8 hores
Avaries greus	3 hores	24 hores
Avaries lleus	8 hores	72 hores
Peticions urgents	4 hores	48 hores
Peticions no urgents	24 hores	5 dies naturals

La categorització i la classificació dels tipus d'incidències.

5. Servei d'assessorament en ciberseguretat

El servei d'assessorament en ciberseguretat esdevindrà en una auditoria inicial per entendre l'estat en què es troba l'ens local. Aquesta auditoria permetrà identificar les vulnerabilitats i riscos presents en tota la infraestructura. A partir d'aquesta avaluació, es generarà un Pla de Millora, que inclourà recomanacions per millorar la ciberseguretat i millorar el compliment normatiu. Un cop lliurat el Pla de Millora, es realitzarà un seguiment i supervisió mínima d'un any per assegurar la correcta implementació i evolució de les mesures proposades, garantint una millora contínua de la ciberseguretat de l'ens. Tot seguit es detallen les fases amb més detall:

Primera reunió presencial:

- Objectiu: El director de projectes i serveis, l'assessor d'administracions públiques, auditor de ciberseguretat, tècnic especialista en ciberseguretat i el personal tècnic de l'ens local, es reuniran en aquesta primera reunió per acordar persones de contacte, canals de comunicació i fixar dates d'execució i entrega d'informe final.
- Canals de comunicació: Es definiran els canals per comunicar les incidències. Seran utilitzats els canals estipulats en el punt 3 segons la gravetat i importància d'aquestes.
- Persones de contacte: S'establirà l'interlocutor principal a l'ens local (responsable tècnic) i també la persona de contacte d'AVENTEC en cas d'incidència, dubtes o suggeriments durant tot el procés. Serà assignada una persona responsable per a cada una de les banda per agilitzar la comunicació.
- Abast de les proves: Es delimitaran quines instal·lacions, sistemes i equips seran revisats i auditats.
- Data inici recollida de dades: S'establirà la primera data per dur a terme les primeres proves a l'ens local. També, s'establirà la freqüència de les següents recollides tenint en compte la naturalesa de l'ens i les preferències del responsable tècnics del propi ens. La temporalitat i l'abast detallat de cada una d'aquestes actuacions es definirà de manera personalitzada després de la primera reunió de coordinació amb l'ens local. Entenem que la naturalesa específica de cada entitat (el seu volum de dades, la complexitat de la seva infraestructura o la seva classificació com a operador de serveis essencials) requerirà una planificació ajustada i adaptada a la seva realitat particular.
- Horari de les proves: Es fixarà un horari per realitzar les proves de forma controlada per evitar que aquestes interfereixin en el dia a dia ni afectin el normal funcionament dels serveis de l'entitat. Abans d'iniciar les proves es contactarà amb el responsable tècnic de l'ens per comunicar-li l'inici de les proves mitjançant els canals pactats.

Recollida d'informació inicial:

- Objectiu: L'objectiu és documentar de manera exhaustiva els components hardware (equips físics), software (programes informàtics) i les configuracions de xarxa presents a l'ens local. Aquesta documentació permetrà establir una base de coneixement sòlida per a les fases posteriors de l'auditoria. Es busca comprendre com s'utilitzen els sistemes informàtics en el dia a dia de l'organització, incloent els fluxos de treball, els usuaris principals i les interaccions amb les diferents aplicacions i serveis. Això proporcionarà un context operatiu essencial per a l'anàlisi.
- Participants claus: Auditor de ciberseguretat i el personal tècnic ens local.

Recollida d'evidències:

- Objectiu: S'obtindran proves concretes de com estan configurats els ordinadors, servidors i altres equips. Això inclou veure quines versions de programari tenen instal·lades, com estan definits els permisos d'accés, estat de les copies de seguretat, encriptació d'informació sensible i quines mesures de seguretat perimetral estan activades. És vol recollir proves que demostrin l'existència de punts febles o punts de millora. Això pot ser una captura de pantalla d'una configuració incorrecta, un registre que mostri un error o un informe que identifiqui un problema. Aquestes evidències són fonamentals per explicar les nostres conclusions i recomanacions.
- Canals de comunicació: El Director de Projectes i Serveis mitjançant un correu electrònic i trucada telefònica es comunicarà amb el responsable tècnic de l'ens. En aquesta comunicació es facilitarà els noms i càrrecs dels auditors de ciberseguretat que duran a terme les proves i

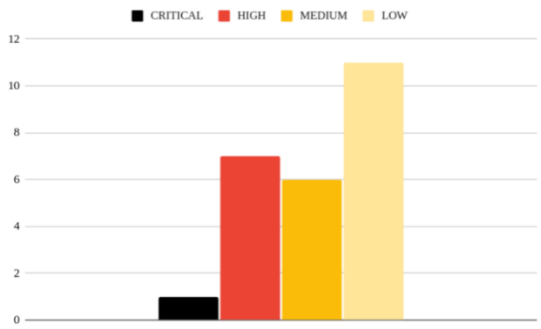
recolliran la informació. També, es concretarà la data, la durada estimada de les proves i s'especificarà exactament quins actius seran auditats de tots els possibles.

- Participants claus: El responsable tècnic de l'ens local podrà comunicar-se mitjançant establerts amb el director de projecte per comunicar qualsevol incidència o dubte sobre les proves que es durant a terme. Tanmateix, durant les proves, que sempre seran presencials, també es podrà contactar directament amb l'auditor de ciberseguretat designat prèviament.
- Abast de les proves: Només seran avaluats aquells actius que hagin estat definits a la primera reunió i especificats prèviament pel director de projectes. Qualsevol modificació o ampliació dels mateixos haurà de ser comunicat per escrit al responsable tècnic de l'ens local, i posteriorment es realitzaran els canvis necessaris a l'auditoria / servei.
- Comunicació d'incidents durant l'auditoria: No és objectiu de l'auditoria realitzar una interrupció a la normal operació de l'ens local, però existeix la possibilitat que per error humà o error tècnic es produeixi una interrupció o incidència sobre l'actiu que s'està auditant. En aquest cas, el protocol serà directe i precís. En cas de detectar un incident degut a les proves que s'està duent a terme, l'auditor de ciberseguretat immediatament es comunicarà amb el responsable tècnic de l'ens local i posteriorment amb el director de projectes. AVENTEC col·laborarà tècnicament amb tot el que sigui necessari per a restablir el servei i oferirà suport tècnic, administratiu i assessorament per resoldre l'incident. Posteriorment, aquest incident serà documentat en l'auditoria per tal d'avaluar-ho en l'informe final.
- Horari de les proves: A causa de la naturalesa de les proves, aquestes hauran de ser realitzades en horari laboral i de forma presencial a les instal·lacions designades. Entenen la criticitat d'aquestes proves el responsable tècnic de l'ens serà coneixedor en tot moment de les proves que es realitzaran.

Informe de troballes i Pla de Millora

- Objectiu: Presentar un informe clar i precís de les debilitats, mancances, vulnerabilitats i riscos identificats. Juntament amb l'informe, es presentarà un pla de millora. Aquest pla de millora s'alinearà amb les bones pràctiques i els requisits de seguretat establerts en l'Esquema Nacional de Seguretat (ENS) i tindrà en compte les directius de la normativa NIS2. L'objectiu final és que les millores proposades no només siguin efectives, sinó que també ajudin amb els marcs legals actuals.
- Canals de comunicació: La reunió per a la presentació de l'informe es convocarà amb antelació suficient mitjançant un correu electrònic formal. Aquest correu detallarà la data, l'hora, el lloc i l'ordre del dia de la reunió. La presentació de l'informe i la discussió del Pla de Millora es realitzaran sempre de forma presencial. Entenem que la presencialitat facilita la comprensió, la resolució de dubtes i l'estableix un diàleg més fluid. Només en cas que el responsable tècnic de l'ens local ho sol·liciti explícitament i ho consideri convenient, la reunió es podrà dur a terme de forma telemàtica.
- Participants claus: Per part d'AVENTEC; el Director de projectes i serveis, l'assessor d'administracions públiques i ens locals, i el personal tècnic que ha participat en l'auditoria. En el cas de l'ens local; el responsable tècnic i el responsable polític de l'àrea afectada (si s'escau). Qualsevol altre membre de l'equip que es consideri rellevant per entendre els resultats i les implicacions del pla de millora.
- Contingut de l'informe:
    - **Part Executiva**: Aquesta secció serà un resum dels punts més importants de l'auditoria. Presentarà les conclusions generals sobre l'estat de la infraestructura

digital, destacant els principals riscos i les oportunitats de millora. No inclourà tecnicismes, sinó que es centrarà en l'impacte real que les troballes tenen en el funcionament diari i la seguretat.



Gràfic d'exemple que es pot mostrar en un resum executiu

- **Informe Tècnic**: Aquí es trobarà el detall complet de totes les troballes, amb les evidències recollides durant la fase d'auditoria. Cada punt feble, mancança o vulnerabilitat identificada es descriurà de forma precisa, acompanyada de les proves que ho demostren. Aquesta secció serà més tècnica, però sempre amb una explicació clara de la implicació de cada troballa.
- **Pla d'Acció i Millora**: Aquesta és la secció més important i pràctica. Presentarà les recomanacions concretes i prioritzades per abordar cada una de les troballes. Per a cada recomanació, s'indicarà la gravetat del risc, la prioritat d'implementació i una estimació del temps o l'esforç necessari per portar-la a terme. S'identificaran solucions per prevenir amenaces conegudes com el ransomware, risc de suplantació d'identitat i el phishing. Les propostes de millora estaran basades en les bones pràctiques i els requisits de l'ENS, NIS2 i ISO 27001, assegurant que les solucions encaminen cap a un compliment més robust i una major seguretat. S'establiran persones o àrees responsables per a l'execució de cada acció, facilitant el seguiment. Es proposaran indicadors de seguiment per avaluar l'èxit de les implementacions.

- Establir freqüència de les visites de seguiment: Per assegurar que el Pla de Millora s'implementa de forma efectiva i que qualsevol dubte o dificultat es resol, s'acordarà un calendari de visites de seguiment. La freqüència inicial d'aquestes visites es definirà en la mateixa reunió de presentació de l'informe. L'objectiu és acompanyar l'ens local i garantir que s'entén i s'executa el pla de millora.

Visites de seguiment

- Objectiu: Verificar la correcta implementació de les accions correctores i preventives definides en el Pla de Millora. Proporcionar actualitzacions periòdiques sobre les novetats rellevants en l'àmbit de la ciberseguretat, incloent-hi canvis normatius (revisions de l'Esquema Nacional de Seguretat o la Directiva NIS2), l'emergència de noves amenaces i les millors pràctiques per a la seva prevenció i mitigació
- Canals de comunicació: Les sessions de seguiment es duran a terme amb caràcter presencial, afavorint un diàleg fluid, la resolució immediata de qüestions i la verificació in situ de les implementacions. No obstant això, a instàncies del responsable tècnic de l'ens local, i prèvia avaluació de la seva idoneïtat, aquestes sessions podran ser realitzades mitjançant amb videotrucada.
- Freqüència: La freqüència de les visites de seguiment s'establirà d'acord amb l'ens local en la reunió de presentació del Pla de Millora. Aquesta s'ajustarà a la complexitat de les accions

a implementar i a les necessitats específiques de l'organització, podent ser mensual, bimensual o trimestral. El període mínim de seguiment serà d'un any després de la presentació de l'informe.

- Participants claus: Director de Projectes i Serveis (per part de l'equip auditor), i el personal tècnic de l'ens local descrit anteriorment.

6. Servei de formació en ciberseguretat

Aquest servei té com a finalitat capacitar el personal dels ens locals en matèria de ciberseguretat, aportant coneixements essencials per a la protecció de l'administració pública i, si s'escau, de les infraestructures crítiques que aquesta gestiona. La formació s'estructura en funció del públic al qual va dirigida:

- Formació general: Aquesta formació aborda la identificació i prevenció de riscos digitals com el phishing, infecció per malware i altres amenaces similars. Tanmateix també promou les bones pràctiques en la gestió de contrasenyes, l'ús d'eines digitals segures, i fomenta la conscienciació sobre les últimes amenaces, incloses les derivades de la intel·ligència artificial.
- Formació especialitzada per a responsables TIC: dirigida al personal amb responsabilitats tecnològiques, aquesta modalitat inclou la gestió d'infraestructures segures, la implementació de mesures de seguretat avançades, la capacitació per a la resposta davant incidents de ciberseguretat, i subratlla la importància de les còpies de seguretat per a la recuperació davant desastres. Addicionalment, s'ofereix una actualització sobre normatives rellevants, com la NIS2, el Reglament sobre Intel·ligència Artificial i les regulacions referents de protecció de dades personals.

Tot seguit es detallen les fases amb més detall:

Identificació de necessitats i coordinació inicial

- Objectiu: Comprendre en profunditat les necessitats formatives de cada ens local i definir amb claredat els canals de comunicació i les bases operatives per a una col·laboració efectiva.
- Procés: Es durà a terme una reunió inicial amb els representants designats de cada ens local. Durant aquesta trobada, es tractaran aspectes clau com el nombre estimat de participants per a cada tipus de formació, els perfils professionals a capacitar, les preferències horàries i la disponibilitat de recursos logístics i tecnològics (espais, equipament, connectivitat). Aquesta discussió permetrà determinar la modalitat de formació més adequada i adaptar els continguts si es considera necessari.
- Canals de comunicació: S'utilitzarà principalment el correu electrònic. Durant la reunió, es definiran els canals de comunicació preferents per a les fases posteriors del servei (telèfon, correu electrònic, WhatsApp o altres plataformes).
- Participants clau: Director de Projectes i Serveis, Assessor d'Administracions Públiques i el representant de l'ens local.

Sessions formatives

- Objectiu: Capacitar el personal dels ens locals en ciberseguretat mitjançant la transmissió de coneixements pràctics i aplicables, així com la conscienciació sobre les noves amenaces digitals.
- Freqüència: La freqüència i durada de les sessions es determinaran en la fase de coordinació inicial amb cada ens local, ajustant-se a les seves necessitats i disponibilitat.
- Format de les sessions: Les formacions seran predominantment presencials, llevat que l'ens local opti per la modalitat amb videotrucada. Es prioritzarà un enfocament pràctic i participatiu:

- Simulacions i casos reals: La formació es basarà en casos reals d'incidents per exemplificar amenaces i promoure bones pràctiques. També s'integraran simulacions (presencials o post-sessió), incloent-hi la identificació de phishing, per reforçar l'aprenentatge pràctic.
- Pràctiques per a tècnics: les sessions a part de la teoria Inclouran simulacions i exercicis pràctics directament enfocats a la gestió d'infraestructures segures i a la resposta efectiva davant incidents. S'utilitzaran eines específiques per realitzar autodiagnòstics, es practicarà amb programari de còpies de seguretat per a la recuperació davant desastres, i es formarà sobre els canals oficials per notificar incidents de seguretat greus.

- Accés als continguts en línia: Els continguts exposats durant les sessions estaran disponibles a través d'una plataforma en línia per a la seva posterior consulta i revisió.

Exemple continguts en línia d'un curs d'especialització en ciberseguretat

Seguiment i avaluació

- Objectiu: Consolidar els coneixements impartits i assegurar la seva aplicació pràctica per part del personal. Mitjançant el seguiment es voldrà mantenir el personal actualitzat davant les noves amenaces i l'evolució normativa en ciberseguretat
- Canal de comunicació: Després de la finalització de les sessions formatives, els assistents podran continuar formulant preguntes i consultes a través dels canals de comunicació establerts durant la fase inicial del servei (principalment correu electrònic i telèfon, amb la persona de contacte designada).
- Freqüència: S'establirà un període de suport post-formació inicial durant el qual es prioritzarà la resolució de dubtes. Addicionalment, es podran acordar sessions de recordatori o actualització periòdiques amb l'ens local, amb una freqüència a determinar, segons necessitats, per abordar les noves amenaces o canvis normatius rellevants.

7. Servei de suport integral en ciberseguretat

Aquest servei proporciona una solució completa i adaptable per als ens locals de petita i mitjana grandària. El seu propòsit és oferir una protecció robusta i continuada que cobreixi les necessitats essencials de seguretat digital de l'administració pública.

El servei inclou un ampli ventall d'actuacions, que van des de la millora de la seguretat de xarxes (amb especial atenció a aquelles de sectors crítics que poguessin gestionar), passant per la implementació de sistemes de còpies de seguretat fiables i la planificació de la recuperació davant desastres.

Tanmateix s'ofereix un servei de resposta davant d'incidents greus per tal de restaurar els sistemes després d'un atac de randsomware o pèrdues d'informació. S'utilitzen els mateixos canals de comunicació descrits en l'apartat 3 i el mateix personal proposat en l'apartat 1.