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/la senyor/a RUBEN GARCIA CASTRO com Administrador Solidari (*senyaleu les vostres facultats de representació: per exemple, administrador/a únic/a, apoderat/da,...)*, de l'empresa MAIN MEMORY SA, 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 37, 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.

(Lloc, data i signatura electrònica)

35055393N
RUBEN GARCIA
(R: A58439167)

Firmado digitalmente por 35055393N RUBEN GARCIA (R: A58439167)
Fecha: 2025.05.29 10:21:01 +02'00'

main) memory
technology partner

LOTS 34 a 41. SERVEIS DE CIBERSEGURETAT

Prestació 172. Servei d'assessoria en ciberseguretat
Prestació 173. Servei de formació general en ciberseguretat

Contenido

1. PRESENTACIÓ DE MAIN MEMORY

MAIN MEMORY, S.A. és una companyia d'assessoria i serveis en tecnologies de la informació amb infraestructura pròpia a Espanya i cobertura a nivell nacional.
Som experts en la integració de tecnologies i de comunicacions, amb un component afegit de mobilitat i d'identificació automàtica; tot assegurat per la nostra experiència de més de 30 anys en solucions i serveis tecnològics per a diversos sectors.

Outsourcing

- Consultors.
- Cap de projectes.
- Analistes.
- Programadors.
- Tècnics de Sistemes.

Consultoria

- Consultoria tecnològica.
- Disseny i implantació de Sistemes a mida en diferents plataformes (IBM, Wintel...)
- Implantació de solucions d'RFID.
- Disseny i implantació de solucions SGA.
- Solucions de mobilitat i veu.

Seguretat

- Auditoria de seguretat.
- Serveis Disaster Recovery Planning.
- Centre de Backup alternatiu.
- Alta disponibilitat.
- Hosting d'alta disponibilitat.

Manteniment Hardware/Software

- Manteniment HW & SW, Preventiu i correctiu.
- Gestió de las Garanties y Contractes Externs.

Instal·lació, administració i integració de sistemes

- OS/400
- Entorn Windows
- Unix/AIX
- Interfícies corporatives
- Virtualització

IBM Series

- Administració de sistemes (local y remotament)
- Capacity planning
- Configuracions LPAR, Consolidació de sistemes
- Formació en Iseries
- Seguretat perimetral (ODBC, FTP, etc.) i interna OS/400
- Comunicacions
- Websphere

Sistemes d'identificació automàtica

- Radio WiFi.
- RFID.
- Terminals de ma, Terminals de vehicles, Punts d'accés, impressores de codis de barres, etc.

Infraestructures

- Projectes d'instal·lació.
- Manteniment de xarxes, cablejades i infraestructura de dades/elèctrica.
- Certificació; proba de l'equipo de comprovació y documentació acreditativa del test.
- Documentació de la obra; esquema/s del recorregut del cable, ubicació dels punts, armaris i quadres elèctrics
- Auditoria de tràfic de xarxa.

MAIN MEMORY: Solucions professionals 24x7

- Presencia nacional
- Independència del fabricant
- Cobertura 24x7, alta disponibilitat en 24x7
- Intervencions On Site i/o intervencions remotes
- Compromís de mitjans
- Tècnics Especialistes, Enginyers i consultors.
- Certificacions Tècnica (Dpt. Tècnic, de Consultoria i Enginyeria).
- Service Desk Centralitzat(CO).
- Dotacions en recanvis / Logistica Multi-Magatzem.
- Laboratoris tècnics.
- Sistemes Integrats en Gestió d'Operacions.
- Plataformes Mutualitzades de Suport a Usuaris i Sistemes.

Per què Main Memory?

Un cop aconseguits els nostres primers trenta anys, des de MAIN MEMORY, S.A. desitgem compartir el nostre entusiasme de tornar la vista enrere i carregar-nos de forces per mirar el futur positivament.
Des del 1987, any en què iniciem la nostra activitat, la Tecnologia ha facilitat la nostra feina i la qualitat de vida professional dels nostres clients i associats; més de trenta anys de consolidació continuada en l'evolució de l'entorn tecnològic corporatiu.
El nostre propòsit ferm és fer més senzilla la vida professional.

Tot i així, aquests anys ens permeten tenir la perspectiva suficient per observar que el que és realment important per aconseguir els objectius comuns –els dels nostres clients i els nostres- és important envoltar-se de persones; persones capacitades que ens facin millors a tots – no sols per les seves aptituds sinó també per la seva actitud i implicació- les quals ens permeten dirigir-nos cap al futur amb satisfacció.

MAIN MEMORY, S.A. aporta els beneficis següents:

- Experiència en el disseny, implantació i manteniment de nombrosos projectes en els darrers trenta anys.

- Capacitat d'integració i adaptació a l'activitat de negoci de les empreses amb què col·laborem. A MAIN MEMORY, S.A. assumim com a nostres els reptes tecnològics que ens plantegen els nostres clients.

- Estratègia activa de seguiment del negoci per aportar idees complementàries a les funcionalitats presents i futures.

- Coordinació i control d'efectius i activitats a dur a terme mitjançant una estructura organitzativa de la direcció de projectes.

- Formació tecnològica continuada dels recursos propis redundant en més eficàcia i efectivitat de cara als nostres clients.

2. SERVEI D'ASSESSORIA EN CIBERSEGURETAT

Proposta d'Auditoria, Consultoria i Pla de Millora

1. Introducció

La seguretat de la informació s'ha convertit en una prioritat estratègica per a totes les organitzacions, especialment en un context de creixent digitalització i increment de les ciberamenaces. Tant els atacs de ransomware com el phishing, el robatori d'identitats o les vulneracions de dades poden tenir conseqüències devastadores a nivell econòmic, legal i reputacional. En aquest entorn, el compliment normatiu (com el marc ENS o la Directiva NIS2) no només és una obligació legal, sinó una garantia de resiliència i confiança.

Amb aquesta proposta de servei, oferim una **assessoria integral en ciberseguretat**, estructurada en dues fases clau:

1. Auditoria i consultoria inicial.
2. Disseny i desenvolupament d'un Pla de Millora a mida.

Als propers apartats es detallaran algunes tasques habituals que poden encabir-se dintre dels serveis oferts però serà en fases posteriors i en negociacions amb cadascun dels ENS que sol·licitin el servei, os es definiran les tasques sol·licitades i els requeriments finals en volum d'hores necessàries.

2. Fase 1: Auditoria i Consultoria Inicial

2.1 Objectiu

L'objectiu d'aquesta primera fase és obtenir una comprensió clara, profunda i objectiva de la situació actual de l'organització en matèria de seguretat de la informació i identificar possibles punts febles que podrien comprometre la disponibilitat, integritat i confidencialitat de les dades.

2.2 Activitats previstes

2.2.1 Auditoria tècnica de la infraestructura

- Avaluació de servidors, xarxes, sistemes operatius i dispositius d'emmagatzematge.
- Identificació de vulnerabilitats en components de maquinari i programari.
- Detecció de ports oberts, serveis exposats i configuracions insegures.

- Anàlisi de vulnerabilitats conegudes (CVEs) amb eines de tipus vulnerability scanner.

2.2.2 Revisió de polítiques i processos

- Estudi dels protocols de seguretat establerts.
- Revisió de l'existència i aplicació de polítiques de gestió d'identitats, control d'accés, gestió d'incidents i còpies de seguretat.
- Validació de l'aplicació de mesures d'encriptació de dades en repòs i en trànsit.

2.2.3 Anàlisi de controls d'accés i gestió d'usuaris

- Verificació dels mecanismes d'autenticació (autenticació multifactor, contrasenyes robustes, SSO).
- Revisió del cicle de vida dels usuaris i gestió de privilegis.
- Avaluació del nivell de segregació de funcions i mínim privilegi.

2.2.4 Avaluació de la cultura i conscienciació en ciberseguretat

- Entrevistes o enquestes als empleats per detectar el nivell de sensibilització sobre riscos com phishing o enginyeria social.
- Revisió de programes de formació i simulacres d'incidents (si existeixen).

3. Fase 2: Pla de Millora

3.1 Objectiu

Amb la informació obtinguda en la fase anterior, s'elabora un Pla de Millora personalitzat que permeti corregir vulnerabilitats detectades, elevar el nivell de seguretat de l'organització i garantir el compliment normatiu. Aquest pla es presenta com un full de ruta progressiu, prioritzat i escalable.

3.2 Contingut del pla

3.2.1 Recomanacions tècniques

- Substitució o reforç dels sistemes vulnerables.
- Implementació de tallafocs de nova generació (NGFW), sistemes de detecció i prevenció d'intrusions (IDS/IPS), i solucions de seguretat perimetral.
- Migració a serveis amb major suport de seguretat.

3.2.2 Estratègies de protecció davant ciberamenaces

- Solucions específiques contra ransomware: segmentació de xarxa, còpies de seguretat automatitzades, eines EDR (Endpoint Detection and Response).
- Protecció contra phishing: filtres avançats de correu, solucions anti-spam, simulacions de phishing per formar el personal.
- Monitorització constant: implementació de SIEM (Security Information and Event Management) per a una detecció precoç de comportaments anòmals.

3.2.3 Millores organitzatives i formatives

- Creació o actualització de polítiques de seguretat.
- Implementació d'un pla de resposta a incidents i un centre d'operacions de seguretat (SOC).
- Formació periòdica al personal en bones pràctiques, reconeixement de ciberamenaces i protocols d'actuació.

3.2.4 Compliment legal i normatiu

- Desenvolupament de mesures IT per al compliment dels requisits de:
    - **ENS (Esquema Nacional de Seguretat)**: classificació dels sistemes, mesures bàsiques, mitjanes i altes, gestió de riscos i seguretat per disseny.
    - **NIS2**: avaluació de riscos sistèmics, responsabilitat del lideratge, notificació d'incidents i protecció de la cadena de subministrament.
    - Altres normatives aplicables com **ISO 27001** entre d'altres.

4. Beneficis del Servei

El servei d'assessoria en ciberseguretat que proposem té múltiples avantatges per a la teva organització:

- **Millora de la resiliència** davant atacs informàtics i reducció del risc operatiu
- **Compliment amb normatives exigides**, evitant sancions i millorant la imatge corporativa.
- **Optimització de recursos**, prioritzant inversions en seguretat on realment cal.
- **Augment de la confiança** per part de ciutadans i proveïdors.
- **Professionalització de la gestió de riscos tecnològics**, alineant tecnologia i estratègia.

5. Metodologia i Cronograma Proposat

5.1 Metodologia

El servei es basa en metodologies reconegudes com el cicle **PDCA (Plan-Do-Check-Act)**, l'enfocament **risk-based thinking** i l'ús d'eines automatitzades i auditories manuals.

5.2 Etapes i durada estimada

Etapa	Durada estimada
Recollida d'informació	1 setmana
Auditoria tècnica i documental	2-3 setmanes
Elaboració d'informe inicial	1 setmana
Disseny del Pla de Millora	1-2 setmanes
Presentació i validació	1 setmana

Durada total estimada: **6 a 8 setmanes**

6. Conclusions

El nostre servei d'assessoria en ciberseguretat ofereix una visió estratègica i tècnica completa per ajudar a les organitzacions a avançar cap a un entorn més segur, resilient i conforme amb la normativa vigent. La combinació d'auditoria, consultoria experta i elaboració d'un pla de millora permet abordar tant els aspectes tècnics com organitzatius de la seguretat.

Aquest servei és especialment recomanable per Administracions públiques degut a que disposen d'infraestructures crítiques, tenen requisits normatius estrictes com el ENS i es troben en ple procés de transformació digital.

3. SERVEI DE FORMACIÓ GENERAL EN CIBERSEGURETAT

Proposta de formació General i per a responsables TIC

1. Objectiu i justificació

L'evolució de les tecnologies de la informació i la comunicació (TIC) ha comportat un increment exponencial dels riscos associats a l'ús de sistemes digitals. Les amenaces cibernètiques afecten tant entitats privades com administracions públiques, i sovint tenen conseqüències greus com el robatori de dades, la interrupció de serveis essencials o la pèrdua de confiança ciutadana.

En aquest context, la formació contínua en ciberseguretat és una eina fonamental per a la prevenció i la resiliència. Aquesta prestació té com a objectiu capacitar els treballadors i responsables TIC de l'ens contractant en matèria de seguretat digital, mitjançant accions formatives adaptades al nivell d'exposició i responsabilitat dels diferents perfils professionals.

La formació es divideix en dues línies principals:

- Formació general en ciberseguretat, dirigida a tot el personal.
- Formació especialitzada per a personal tècnic i responsables de seguretat TIC.

Als propers apartats es detallaran continguts habituals que poden encabir-se dintre de les formacions ofertes però serà en fases posteriors i en negociacions amb cadascun dels ENS que sol·licitin el servei, os es definiran, si fa falta, formacions especifiques.

2. Servei de Formació General en Ciberseguretat

a. Finalitat

Dotar el personal no tècnic de coneixements bàsics en matèria de seguretat digital per tal de:

- Identificar situacions de risc.
- Prevenir accions que puguin comprometre la seguretat de la informació.
- Fomentar una cultura organitzacional de responsabilitat digital.

b. Continguts detallats

i. Amenaces habituals en l'entorn digital:
   1. Phishing, spear phishing i smishing: tècniques de frau mitjançant correu electrònic, SMS o xarxes socials.
   2. Malware, ransomware i troians: funcionament, vies d'entrada i conseqüències.
   3. Enginyeria social: manipulació psicològica per obtenir informació confidencial.
   4. Amenaces internes: negligència, mala configuració o errors humans que poden generar bretxes de seguretat.

ii. **Pràctiques de seguretat personal:**

1. Creació i gestió segura de contrasenyes: sistemes de verificació en dos passos (2FA/MFA), ús de gestors de contrasenyes.
2. Navegació segura: identificació d'URLs falses, verificació de certificats digitals.
3. Ús responsable del correu electrònic i de les plataformes col·laboratives.
4. Gestió d'informació sensible i confidencial: criteris de classificació i compartició.

iii. **Protecció de dispositius:**

1. Actualitzacions periòdiques de sistemes operatius i programari.
2. Antivirus i firewalls personals.
3. Bones pràctiques en dispositius mòbils i teletreball.

iv. **Conscienciació a través d'exemples pràctics:**

1. Estudi de casos reals d'incidents cibernètics en entitats públiques.
2. Simulacions de correus fraudulents i resolució d'exercicis pràctics.

v. **Metodologia**

1. Sessions dinàmiques, adaptades a diferents nivells i perfils.
2. Utilització de metodologies participatives: role playing, gamificació, resolució de casos.
3. Possibilitat d'execució en format presencial, virtual o híbrid.
4. Avaluació final mitjançant qüestionaris interactius.

vi. **Resultats esperats**

1. Increment de la capacitat de detecció d'amenaces per part del personal.
2. Reducció dels incidents derivats d'errors humans.
3. Millora generalitzada de l'actitud proactiva davant la seguretat.

3. Formació Especialitzada per a Responsables TIC

a. Finalitat

Capacitar els responsables tècnics en la gestió integral de la seguretat de les infraestructures tecnològiques, amb coneixements avançats sobre eines, normatives i procediments específics.

b. Continguts detallats

i. Gestió de la seguretat TIC:

1. Disseny i desplegament d'arquitectures segures.
2. Segmentació de xarxes i aplicació del principi de mínim privilegi.
3. Configuració segura de sistemes operatius, bases de dades i aplicacions.
4. Monitorització contínua i sistemes de registre i traçabilitat (logs).

ii. Resposta davant incidents de seguretat:

1. Etapes d'un pla de resposta: detecció, contenció, erradicació, recuperació i aprenentatge.
2. Tipologies d'incidents (DoS, exfiltració de dades, intrusions).
3. Comunicació efectiva amb els equips de gestió, autoritats i usuaris afectats.
4. Elaboració d'informes postincident.

iii. Mesures de seguretat avançades:

1. Sistemes de prevenció i detecció d'intrusions (IDS/IPS).
2. Sistemes de gestió d'identitats (IAM) i autenticació forta.
3. Còpies de seguretat segures i plans de recuperació davant desastres (DRP).
4. Xifratge d'informació en trànsit i en repòs.

iv. Compliment normatiu:

1. Adaptació a l'Esquema Nacional de Seguretat (ENS): nivells bàsics, mitjans i alts, controls tècnics i organitzatius.
2. Coneixement de la LOPDGDD i RGPD: tractament de dades personals, principis de responsabilitat proactiva.
3. Directiva NIS2: aplicació a serveis essencials i gestió de riscos.
4. Implantació i manteniment de Sistemes de Gestió de la Seguretat de la Informació (SGSI) segons ISO/IEC 27001.

c. Metodologia

i. Cursos amb enfocament pràctic.

d. Certificació

i. Certificació d'assistència

4. Modalitat de prestación

a. Adaptació flexible segons les necessitats de l'ens: formació puntual, programes anuals, tallers temàtics.
b. Possibilitat de crear itineraris formatius per rols professionals específics.

5. Beneficis globals per a l'organització

- Millora del nivell global de seguretat digital.
- Compliment més robust dels marcs legals i normatius.
- Reducció del risc d'incidents greus i minimització de l'impacte.
- Sensibilització de tota l'organització envers la ciberseguretat com a valor essencial.

IT Works

Barcelona
Ramis, 16
08012 Barcelona
T 93 213 96 98

Madrid
López de Hoyos, 155
3ª Planta, Puerta 1
28002 Madrid
T 91 459 92 90

Valencia
Mariano de Cavia, 21
46014 Valencia
T 96 356 41 82

902 467 467
info@mainmemory.es
www.mainmemory.es

main memory
technology partner

Main Memory, S.A. | A58439167
Registro Mercantil de Barcelona, tomo 8.908, libro 8.138, sección 2a, folio 196, hoja 104.477, inscripción 1a