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

52155234C
JOSE LUIS RUS
(R: B64161250)

Firmado digitalmente por 52155234C JOSE LUIS RUS (R: B64161250)
Fecha: 2025.05.29 10:34:29 +02'00'

**TECNICA LOT 38 - SERVEIS DE CIBERSEGURETAT – ÀMBIT PONENT**

Client: Consorci Català pel Desenvolupament Local
Expedient: 2024.01
Data: 29/05/2025
Versió: v1

C/ Esteve Terrades, 58
08402 Granollers (BCN)
M. 656 391 871 · T. 902 012 813
www.puntinformatic.com

## Índex

# 1. Coordinació amb l'entitat local

## 1.1 Mecanismes de coordinació i comunicació

Per assegurar una coordinació efectiva amb l'entitat local contractant durant tota la prestació del servei, es proposa establir diversos mecanismes de comunicació i coordinació i els seus responsables . Aquests inclouen:

### 1.1.1 Responsables

- **Responsable de servei**: Es designarà un responsable de servei que actuarà com a punt de contacte principal entre l'entitat local i el nostre equip. Aquest responsable supervisarà la prestació del servei, coordinarà les reunions, elaborarà els informes, controlarà el compliment dels SLA's i garantirà que totes les incidències siguin resoltes de manera eficient i dins del termini establert.

- **Responsable tècnic**: Es nomenarà un responsable tècnic que s'encarregarà d'implementar les pràctiques adequades de manteniment segons la tecnologia, redefinir arquitectures i donar suport al responsable de servei en la elaboració de plans de millora i propostes d'evolució tecnològica.

### 1.1.2 Reunions de seguiment

Es duran a terme diferents reunions periòdiques amb els responsables de l'entitat local per revisar l'estat dels serveis de manteniment i monitorització, discutir les incidències, planificar futures accions, revisar els indicadors de qualitat i abordar millores tecnològiques i procedimentals. Aquestes reunions permetran una comunicació efectiva i una resolució ràpida de qualsevol problema que pugui sorgir.

Durant la prestació del servei, es preveuen les següents sessions o reunions mínimes:

- **Reunió inicial**: Una reunió de kickoff per establir els objectius, les expectatives i els procediments de treball. Aquesta reunió permetrà definir clarament els objectius del projecte i assegurar que totes les parts estiguin alineades.
- **Reunions setmanals**: Reunions de seguiment setmanals per revisar l'estat dels serveis, discutir incidències i planificar accions correctives. Aquestes reunions permetran una comunicació constant i una resolució ràpida de qualsevol problema que pugui sorgir.
- Possibles millores. Aquestes reunions permetran una avaluació detallada de la qualitat del servei i identificar oportunitats de millora a llarg termini.

### 1.1.3 Canals de comunicació

Es posaran a disposició diversos canals de comunicació per a la gestió d'incidències, incloent correu electrònic, telèfon mòbil i una línia telefònica dedicada. A més, es facilitarà l'accés a una plataforma de gestió de tiquets per registrar i seguir les incidències. Aquesta plataforma permetrà una gestió eficient de les incidències, assegurant que totes les sol·licituds siguin ateses de manera oportuna.

Per a la gestió d'incidències, es proposa utilitzar els següents canals de comunicació:

- **Correu electrònic**: Un correu electrònic dedicat per a la recepció i gestió d'incidències. Aquest canal permetrà obrir tickets directament a la plataforma de gestió de tickets, afavorint una comunicació ràpida i eficient. Això garantirà que totes les sol·licituds siguin ateses de manera oportuna i que no es perdi cap informació.
- **Línia telefònica dedicada**: Una línia telefònica dedicada per a la gestió d'incidències crítiques. Aquest canal permetrà una comunicació directa i immediata en cas d'incidències que requereixin una atenció urgent.
- **Telèfon mòbil del coordinador:** Aquesta via de comunicació ajuda a mantenir una relació propera amb el responsable del servei per parlar de temes operatius o per escalar algun assumpte urgent que el client consideri necessari.
- **Plataforma de gestió de tiquets**: Una plataforma en línia per registrar, seguir i gestionar les incidències. Aquesta plataforma permetrà una gestió eficient de les incidències, assegurant que totes les sol·licituds siguin ateses de manera oportuna. Aquesta plataforma esta activa 24/7.

## 1.2 Prestació 172. Servei d'assessoria en Ciberseguretat

### 1.2.1 Auditoria i consultoria inicial

#### *1.2.1.1 Auditoria seguretat interna*

El Test d'Intrusió Intern permet als auditors simular un atac des de dins de l'empresa, per exemple, un ciberdelinqüent que ja hi hagi obtingut accés, un treballador descontent, etc. Així, doncs, l'auditor podrà disposar de credencials d'accés al sistema (sense privilegis), accés a la xarxa corporativa (LAN), etc.

El Test d'Intrusió es fa seguint les metodologies basades en les millors pràctiques, l'objectiu principal és "simular un usuari intern amb permisos Standard i escalar privilegis i vulnerar la infraestructura o els serveis de l'empresa". Els auditors utilitzaran la superfície d'atac més oportuna per a cada cas, per tant l'auditoria se centrarà en els punts amb més risc, provant i obtenint evidències de les vulnerabilitats trobades. Per això s'utilitzaran tècniques com les següents:

Hacking ètic actiu:

- Descobriment de dispositius, xarxes, serveis i protocols mitjançant tècniques automàtiques i posterior validació i revisió manual
- Anàlisi de vulnerabilitats de serveis interns mitjançant tècniques automàtiques i posterior verificació de les vulnerabilitats manual
- Test de força bruta de serveis interns
- Anàlisi de segmentació de xarxa i accessos no autoritzats
- Intent d'explotació de vulnerabilitats trobades
- Test de fuga d'informació

Realització d'informes executiu i tècnic:

- Objectiu, abast, metodologies i fases seguides.
- Resum executiu amb les conclusions més significatives ordenades per criticitat i estatus.
- Informe tècnic amb detall de l'auditoria. Dades tècniques, vulnerabilitats ordenades per criticitat, evidències i recomanacions per resoldre o minimitzar el risc.
- Detall de tasques realitzades.

#### *1.2.1.2 Auditoria seguretat externa*

El test d'intrusió extern realitzat en modalitat Blackbox (sense informació de la infraestructura o serveis a auditar, amb excepció del domini o IP acordats), permet revisar i intentar comprometre la seguretat de l'empresa, centrant-nos en el domini i IP seleccionades.

El test d'intrusió es realitza seguint les metodologies basades en les "best practices", l'objectiu principal és simular un actor extern que pretén vulnerar la infraestructura o serveis per aconseguir posar en risc la informació de l'empresa" utilitzant la superfície d'atac més oportuna per a cada cas. És per aquest motiu que l'auditoria estarà centrada en els punts amb més risc, provant y obtenint evidències de les vulnerabilitats trobades. Per a aconseguir aquest objectiu s'utilitzaran tècniques com les següents:

Hacking ètic passiu i obtenció d'informació externa mitjançant:

- Descobriment de publicació d'informació sensible.
- Test d'indexació de servidors i serveis públics en fonts obertes.
- Test de "Information disclosure" amb motor de cerca Hacking.
- Tècniques de "E-mail Assumption".

Hacking ètic actiu

- Descobriment de dispositius, xarxes, serveis i protocols mitjançant tècniques automàtiques i posterior validació i revisió manual.

- Anàlisi de vulnerabilitats de serveis externs mitjançant tècniques automàtiques i posterior verificació de vulnerabilitats.
- Intent d'explotació de vulnerabilitats trobades.
- Test de servidors DNS amb Wildcarding de DNS/Zones Transfer Test.
- Test de reputació IP dels servidors.
- Test de força bruta de serveis publicats.
- Test d'accés mitjançant xarxes d'anonimat (Tor, I2P, etc).
- Test de bypass de seguretat perimetral (Firewall / IDS / IPS).
- Auditoria de seguretat bàsica de l'entorn web (no exhaustiva).

Realització d'informes executiu i tècnic

- Objectiu, abast, metodologies i fases seguides.
- Resum executiu amb les conclusions més significatives ordenades per criticitat i estatus.
- Informe tècnic amb el detall de l'auditoria. Dades tècniques, vulnerabilitats ordenades per criticitat, evidències i recomanacions per solucionar o minimitzar el risc.
- Detall de tasques realitzades.

### 1.2.2 Pla de millora

Objectiu

Establir un conjunt d'accions estructurades per corregir les deficiències detectades durant l'auditoria de seguretat i reforçar el nivell de protecció dels sistemes, dades i processos de l'organització.

Fases del pla de millora

1. Anàlisi dels resultats de l'auditoria

- Revisió detallada dels informes d'auditoria.
- Classificació de les troballes per:
  - Tipus (tècniques, organitzatives, normatives).
  - Grau de risc (alt, mitjà, baix).
  - Compliment normatiu (ISO 27001, ENS, RGPD, NIS2...).
- Identificació de les causes arrel (root cause analysis).

2. Priorització i planificació de les accions

- Assignació de nivells de criticitat.
- Establiment d'un calendari de correcció:
  - Immediates: comptes amb privilegis innecessaris, serveis exposats.
  - Curt termini: implementació de controls bàsics, revisions de configuració.
  - Mitjà termini: actualització de polítiques, plans de formació.
  - Llarg termini: projectes estructurals, noves eines de seguretat.
- Designació de responsables per a cada acció.

3. Execució de les accions correctives i preventives

- Correcció de vulnerabilitats tècniques (configuració, actualitzacions, canvis d'arquitectura).
- Revisió i actualització de procediments de seguretat.
- Establiment o millora del sistema de gestió de seguretat (SGSI).
- Implantació de controls addicionals (MFA, segmentació, xifrat...).
- Inclusió de mesures preventives per evitar la repetició d'errors.

4. Formació i sensibilització

- Formació específica per a equips TIC segons les troballes.
- Sessions de conscienciació per a usuaris finals (si escau).
- Inclusió de les lliçons apreses a futurs programes de formació interna.

5. Seguiment i verificació

- Definició d'indicadors clau (KPIs) i mètriques de seguiment.
- Revisions periòdiques de l'estat de les accions.
- Avaluació de l'eficàcia de les mesures implementades.
- Realització de reauditories parcials o testos de validació (ex: pentesting, revisió documental).
- Informes de seguiment al comitè de seguretat o a la direcció.

## 1.3 Prestació 173. Servei de formació general en Ciberseguretat

### 1.3.1 Servei de Formació General en Ciberseguretat

Objectiu del pla

Dotar els participants dels coneixements i habilitats necessàries per identificar, prevenir i respondre a amenaces cibernètiques, fomentant una cultura de seguretat digital dins l'organització.

Estructura del pla

El pla es divideix en tres nivells formatius:

1. Nivell bàsic – Sensibilització i bones pràctiques (per a tots els usuaris)

- Què és la ciberseguretat i per què és important.
- Amenaces més comunes (phishing, malware, ransomware, etc.).
- Com crear i gestionar contrasenyes segures.
- Ús segur del correu electrònic i d'internet.
- Prevenció de fugues d'informació.
- Introducció a la normativa de protecció de dades (ex: RGPD).

2. Nivell intermedi – Ciberseguretat aplicada (personal tècnic i operatiu)

- Arquitectura de seguretat bàsica per a xarxes i sistemes.
- Configuració segura de dispositius i serveis.
- Autenticació multifactor (MFA) i control d'accés.
- Gestió de vulnerabilitats i actualitzacions.
- Introducció a sistemes de detecció i resposta (IDS/IPS, SIEM).
- Pràctiques segures en l'administració de sistemes.

3. Nivell avançat – Gestió de la ciberseguretat (comitè directiu, CISO, DPO, etc.)

- Governança de la ciberseguretat i gestió de riscos.
- Elaboració de polítiques i plans de contingència.
- Pla de resposta a incidents i gestió de crisi.
- Marc normatiu i regulatori (ISO 27001, NIS2, ENS, etc.).
- Avaluació de proveïdors i cadenes de subministrament.
- Ciberseguretat en processos de negoci i transformació digital.

Metodologia

- Formació teòrica combinada amb casos pràctics i simulacions.
- Cursos presencials o en línia (format e-learning o webinars).
- Avaluació final per verificar l'assoliment dels coneixements.
- Possibilitat d'incloure simulacres de phishing o proves de penetració per avaluar el nivell de conscienciació real.

### 1.3.2 Formació Especialitzada per a Responsables TIC

Objectiu del pla

Capacitar els responsables TIC perquè puguin dissenyar, implementar i supervisar estratègies de ciberseguretat efectives, alineades amb els objectius de negoci, les normatives vigents i els riscos actuals.

Continguts formatius

1. Marc estratègic i governança de la ciberseguretat

- Rol del responsable TIC en la gestió de la seguretat.
- Elaboració i manteniment del Pla Director de Seguretat (PDS).
- Integració de la seguretat en l'estratègia TIC i de negoci.
- Coordinació amb el CISO, DPO i altres rols clau.

2. Gestió de riscos i anàlisi d'impacte

- Identificació i valoració d'actius crítics.
- Avaluació i classificació de riscos.
- Anàlisi d'impacte en el negoci (BIA).
- Tècniques de mitigació i seguiment del risc.

3. Arquitectura de seguretat i controls tècnics

- Seguretat en xarxes: segmentació, filtratge, VPN, DMZ, NAC.
- Protecció perimetral i interna: firewalls, WAF, EDR/XDR.
- Monitoratge i correlació d'esdeveniments amb sistemes SIEM.
- Control d'accés: gestió d'identitats (IAM), MFA, privilegis mínims.

4. Continuïtat del negoci i resposta a incidents

- Elaboració i prova de plans de continuïtat i recuperació (BCP/DRP).
- Procés de resposta a incidents: detecció, contenció, eradicació i recuperació.
- Coordinació amb equips d'investigació i comunicació de crisi.
- Relació amb CERT/CSIRT i notificació d'incidents.

5. Compliment normatiu i auditories

- Marc legal i normatiu aplicable: RGPD, NIS2, ISO 27001, ENS, LOPDGDD.
- Preparació per a auditories de seguretat i certificacions.
- Elaboració de polítiques, procediments i evidències de compliment.
- Avaluació de tercers i contractes amb proveïdors.

6. Seguretat en entorns actuals

- Seguretat en entorns híbrids i núvol (Azure, AWS, GCP).
- Protecció d'entorns OT/IoT i infraestructures crítiques.
- Amenaces avançades (APT), zero trust i seguretat basada en identitat.
- Intel·ligència de ciberamenaces i anàlisi de tendències.

Metodologia

- Sessions teòrico-pràctiques amb casos reals i enfocament aplicat.
- Tallers tècnics i laboratoris virtuals (hands-on labs).
- Participació en simulacres de crisi cibernètica.
- Avaluació final i lliurament de certificat d'aprofitament.