apdcat
Autoritat Catalana de Protecció de Dades

Plec de prescripcions tècniques per a la contractació del servei d'auditoria interna en l'Esquema Nacional de Seguretat i en la Norma ISO 27001 de Seguretat de la Informació dels sistemes d'informació i de gestió de seguretat de la informació de l'Autoritat Catalana de Protecció de Dades

ACPD-2026-30

Ref. 10.26.2280002

Índex

1. Objecte 2
2. Característiques de l'organització 2
3. Contingut i característiques tècniques generals 3
3.1. Abast del servei 3
3.2. Activitats i lliurables 3
4. Procediment d'auditoria interna 4
4.1. Metodologia general 5
5. Equip de treball 5
6. Calendari d'execució 6
7. Valoració econòmica i contractació 6
Annex: Taula de compliment dels requeriments tècnics i de servei 8

Generalitat de Catalunya

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

1. Objecte

L'objecte d'aquest procediment és la contractació del servei d'auditories internes necessàries per garantir el compliment de l'Esquema Nacional de Seguretat (ENS), d'acord amb el Reial decret 311/2022, i de la Norma UNE-ISO/IEC 27001 de Seguretat de la Informació, Ciberseguretat i Protecció de la Privacitat (ISO/IEC 27001), durant un període de tres anys.

Aquest servei té per finalitat la realització de l'auditoria interna amb caràcter anual, previ a l'auditoria externa efectuada per l'entitat certificadora, ja sigui en el marc d'auditories de seguiment o de certificació, d'acord amb el pla d'auditoria establert.

Les certificacions vigents de l'APDCAT es troben disponibles a UNE-EN ISO/IEC 27001:2012 i ENS.

2. Característiques de l'organització

L'APDCAT és l'organisme independent que garanteix el dret a la protecció de dades personals en l'àmbit del sector públic català i el sector privat que realitza funcions i serveis públics, inclosos els col·legis professionals i les universitats públiques i privades a Catalunya.

Actualment, l'APDCAT compta amb unes oficines situades a la Gran Via de les Corts Catalanes, 635, primera planta a Barcelona, amb 51 llocs de treball.

L'APDCAT disposa d'un Sistema Integrat de Gestió de la Seguretat de la Informació (SIG) certificat conforme a l'Esquema Nacional de Seguretat (ENS) i a la Norma ISO/IEC 27001, amb els objectius següents:

- Complir la normativa vigent relativa a l'obligatorietat de disposar de la certificació de l'ENS, garantint que l'Autoritat compleix els requisits de seguretat exigits.
- Establir i mantenir metodologies òptimes per a la gestió de la seguretat de la informació mitjançant l'aplicació de la Norma ISO/IEC 27001.

La seguretat de la informació constitueix un pilar fonamental per garantir el correcte funcionament d'una administració pública i per generar confiança en la ciutadania respecte dels serveis que presta. Una gestió segura de la informació permet prevenir riscos i vulnerabilitats, així com assegurar la transparència, el compliment normatiu i la reputació institucional.

En aquest context, l'APDCAT és plenament conscient que la informació que tracta és un actiu d'elevat valor, que cal protegir adequadament per garantir-ne la confidencialitat, la integritat i la disponibilitat. Aquests tres principis constitueixen els elements essencials de la seguretat de la informació i són imprescindibles per assegurar aspectes crítics com la continuïtat dels serveis, el compliment de la normativa aplicable i la imatge pública de la institució. La política de seguretat de la informació i la política de protecció de dades de l'APDCAT es troben disponibles al seu lloc web institucional.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

3. Contingut i característiques tècniques generals

L'APDCAT disposa de la certificació vigent conforme a la Norma ISO/IEC 27001 i a l'Esquema Nacional de Seguretat (ENS), en categoria mitjana, aplicables als seus sistemes d'informació i al Sistema Integrat de Gestió de la Seguretat de la Informació (SIG).

3.1. Abast del servei

El servei objecte del contracte comprèn la planificació, execució i tancament de les auditories internes anuals necessàries, prèvies a les auditories externes de seguiment o de renovació/certificació que realitzi l'entitat certificadora, durant un cicle de tres (3) anys.

Així mateix, inclou el lliurament dels informes finals d'auditoria i de tota la documentació associada, incloent-hi els checklists corresponents.

Les auditories internes s'apliquen als sistemes de l'APDCAT següents:

- **Esquema Nacional de Seguretat (ENS)**:

  "Sistemes d'informació que donen cobertura als serveis i les actuacions de l'Autoritat Catalana de Protecció de Dades en l'exercici de les seves competències, en relació amb la ciutadania, les entitats, els organismes i el personal"

- **Norma ISO/IEC 27001 de Seguretat de la Informació**:

  "Sistema de Gestió de la Seguretat de la Informació aplicat als sistemes d'informació que donen cobertura als serveis i les actuacions de l'Autoritat Catalana de Protecció de Dades en l'exercici de les seves competències, en relació amb la ciutadania, les entitats, els organismes i el personal, segons la declaració d'aplicabilitat vigent"

Les auditories internes es realitzaran de manera conjunta i integrada (ENS + ISO/IEC 27001), amb la finalitat d'assegurar una avaluació coherent del SIG i dels sistemes d'informació, evitar duplicitats i garantir la traçabilitat entre requisits normatius i evidències.

3.2. Activitats i lliurables

El servei ha d'incloure, com a mínim, per a cada anualitat, les activitats i lliurables següents:

a) Planificació de l'auditoria interna

- Definició de l'abast, criteris, metodologia, calendari i equips implicats.
- Elaboració i lliurament del Pla d'Auditoria Interna anual, que conté:
  - objectius, abast i referències normatives;
  - agenda, àrees auditades i entrevistes;
  - tècniques d'auditoria i criteris de mostreig;
  - requisits d'evidència i canals de coordinació.

b) Execució de l'auditoria

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

- Recopilació i revisió prèvia de la informació.
- Reunió inicial.
- Revisió documental, entrevistes i verificació d'evidències.
- Avaluació del compliment dels requisits de la Norma ISO/IEC 27001 i de les mesures aplicables de l'ENS.
- Registre de troballes i traçabilitat requisit–evidència.

c) Informe i tancament

- Elaboració de l'Informe d'auditoria interna, que inclourà com a mínim:
  - resum executiu i conclusions;
  - abast i metodologia;
  - no conformitats, observacions i oportunitats de millora;
  - valoració del grau d'implantació i eficàcia del SIG;
  - recomanacions i prioritats.
- Lliurament dels checklists d'auditoria (ENS i ISO/IEC 27001).
- Lliurament de l'informe final d'auditoria, un cop incorporades les consideracions acordades de la reunió de tancament.

d) Seguiment de no conformitats

- Identificació i classificació de no conformitats.
- Revisió del Pla d'Accions Correctives (PAC), amb definició d'accions, responsables, terminis i evidències.
- Suport al seguiment fins a la verificació del tancament, en coherència amb el calendari d'auditoria externa.

La contractació ha de contemplar totes les despeses, incloses desplaçaments i dietes de l'equip auditor.

4. Procediment d'auditoria interna

Les auditories internes objecte d'aquest contracte es realitzaran d'acord amb els principis, requisits i bones pràctiques establerts per l'ENS i de la Norma ISO/IEC 27001, i en particular:

- Pel que fa l'ENS article 31 d'auditoria de seguretat
- Les guies i criteris d'auditoria publicats pel CCN-CERT, especialment els relatius a la verificació del compliment i a la gestió del programa d'auditories que són la CCN-STIC 808 "*ENS. Verificación del cumplimiento*" i la CCN-CERT IC-01/19 "*Criterios generales de auditoría y certificación*"
- La clàusula 9.2 d'Auditoria interna de la Norma ISO/IEC 27001.

L'auditoria interna té com a finalitat:

- Verificar la conformitat del Sistema Integrat de Gestió de la Seguretat de la Informació amb els requisits de l'ENS i de la Norma ISO/IEC 27001;
- Avaluar el grau d'implantació i eficàcia de les mesures de seguretat;
- Identificar no conformitats, observacions i oportunitats de millora;

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

- Contribuir a la millora contínua del sistema, amb caràcter previ a les auditories externes.

4.1. Metodologia general

El procediment d'auditoria interna inclou, com a mínim, les fases següents:

a) **Planificació de l'auditoria**, amb l'elaboració i enviament del Pla d'Auditoria.

b) **Reunió inicial** de l'equip auditor amb els responsables de l'APDCAT per tal d'establir els objectius a cobrir per l'auditoria, verificar dades i revisar la planificació. Aquesta reunió ha de ser presencial i d'acord amb la jornada ordinària de treball de l'APDCAT, en horari de 8.00 a 15.30 hores.

c) **Auditoria**: realització per part de l'adjudicatària de les entrevistes al personal responsable dels processos que corresponguin, així com la realització de visites a les instal·lacions i equipaments de l'APDCAT. Les entrevistes han de ser presencials i d'acord amb la jornada ordinària de treball de l'APDCAT, en horari de 8.00 a 15.30 hores.

d) **Avaluació del compliment** dels requisits aplicables de l'ENS i de la Norma ISO/IEC 27001 i identificació de les possibles no conformitats, observacions i accions de millora.

e) **Reunió final**: L'equip auditor presentarà al personal responsable les conclusions de l'auditoria realitzada, fent l'entrega de l'informe provisional en el mateix moment, on s'especificarà la sistemàtica per a la solució de les no conformitats identificades i de les possibles millores a realitzar.

f) **Lliurament de l'informe final i dels checklists**, en llengua catalana, en el termini màxim de 15 dies des de la realització de l'auditoria.

5. Equip de treball

L'empresa licitadora haurà de tenir els equips auditors qualificats i convenientment acreditats per realitzar els serveis encomanats. L'APDCAT es reserva el dret de sol·licitar les acreditacions pertinents en tot moment.

El contractista haurà d'adscriure a l'execució del contracte els següents mitjans personals:

- Una persona responsable del servei amb categoria mínima d'auditor sènior, la qual haurà de conèixer totes les tasques i serveis inclosos en aquest contracte. Serà, en primer terme, la persona interlocutora amb l'APDCAT i la responsable del servei. També serà la persona encarregada de garantir la qualitat de la prestació del servei i de la coordinació amb l'APDCAT.

  Aquesta persona ha de disposar i complir amb els següents requisits mínims:

  - Certificat com a 'Lead auditor' qualificat, per una entitat certificadora.

  - Coneixement de l'Esquema Nacional de Seguretat i de la Norma ISO 27001. Per això, s'haurà d'acreditar que l'auditor/a responsable disposa d'un mínim de 40 hores de formació específica en la norma i esquema objecte de la contractació.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

- Experiència com a auditor/a responsable o líder en tres (3) auditories de característiques similars a la present contractació, en els últims cinc (5) anys.

- L'equip auditor necessari per portar a terme les auditories de certificació per tal d'optimitzar el temps d'execució del contracte. En cas que el contractista assigni més d'una persona a la realització de les auditories, caldrà assegurar la coordinació entre elles per tal de no repetir les entrevistes als rols claus de l'APDCAT.

6. Calendari d'execució

La planificació del calendari d'execució haurà de respectar les dates i condicionants següents:

- La primera auditoria interna del contracte s'haurà de dur a terme durant el mes de maig de 2026, i l'informe final d'auditoria s'haurà de lliurar en un termini màxim de 15 dies naturals.
- Les dues auditories internes anuals següents es realitzaran, respectivament, durant els mesos de maig de 2027, i maig de 2028.

Les auditories internes objecte del contracte s'hauran de coordinar amb el pla d'auditories externes de certificació i seguiment de l'APDCAT, previst de la manera següent:

- 2026: primer seguiment ISO/IEC 27001
- 2027: renovació certificació ENS i segon seguiment ISO/IEC 27001
- 2028: renovació certificació ISO/IEC 27001

Entre el lliurament de l'informe final d'auditoria interna i la corresponent auditoria externa hi haurà d'haver un termini mínim de 30 dies, amb la finalitat de permetre el tractament adequat de les possibles no conformitats.

L'adjudicatària planificarà i notificarà cada auditoria. En el termini mínim de 2 mesos abans de les auditories, caldrà que contacti amb el responsable del contracte a l'APDCAT per establir un pla d'auditoria que inclogui el cronograma, el pla de treball, la logística i la metodologia de seguiment, així com la coordinació que es portarà a terme. En el termini màxim d'un mes abans de l'auditoria, l'adjudicatària elaborarà i facilitarà a l'APDCAT el Pla d'auditoria.

Les dates concretes de realització de cada una de les auditories es fixaran de mutu acord entre l'adjudicatària i el persona responsable de l'APDCAT. El tractament i resposta que puguin derivar-se de les No Conformitats que l'adjudicatari identifiqui en els sistemes objecte de la present contractació a cada auditoria, s'adequarà per part de l'APDCAT, tant en el termini com en la forma.

7. Valoració econòmica i contractació

Atès que el contracte inclou la realització de tres (3) auditories internes, l'import màxim de licitació per aquest contracte és de 9.000,00 €, IVA exclòs, essent el percentatge a aplicar de l'Impost sobre el valor afegit del 21%, per un import de 1.890,00 €, i que resulta un import total de 10.890,00 €.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

Pressupost	IVA (21%)	Pressupost base licitació
9.000,00€	1.890,00€	10.890,00€

Per tant, el cost del servei d'auditoria interna per anualitat s'estableix en com a màxim: 3.000,00 €, IVA exclòs.

La facturació del servei serà per anualitat, un cop finalitzades totes les tasques corresponent a la o les auditories de l'any corresponent. S'efectuarà un pagament contra factura per a cada anualitat. La factura serà abonada per l'APDCAT dins els terminis legals establerts, una vegada subministrament i comprovat la seva idoneïtat tècnica per part dels responsables de l'Autoritat.

Les entitats recollides a l'article 4 de la Llei 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures del Sector Públic, tindran l'obligació de lliurar la factura que hagin expedit pels treballs i subministraments realitzats per mitjans electrònics.

En la facturació electrònica s'ha de fer constar el codi A09018940 als camps òrgan gestor, unitat tramitadora i oficina comptable (Llei 25/2013).

Les dades de l'APDCAT que han de constar a la factura són les següents:

Autoritat Catalana de Protecció de Dades
Gran Via de les Corts Catalanes, 635, primera planta
08010 Barcelona

Barcelona,

Directora

DILIGÈNCIA: Faig constar que el contingut d'aquest Plec ha estat informat per l'Assessoria Jurídica de l'Autoritat Catalana de Protecció de Dades en data 17 de març de 2026.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.

apdcat
Autoritat Catalana de Protecció de Dades

Annex: Taula de compliment dels requeriments tècnics i de servei

D'acord amb el que s'estableix en el present Plec de Prescripcions Tècniques, i amb l'objectiu de facilitar la verificació del compliment dels requisits mínims exigits, els licitadors hauran d'adjuntar obligatòriament la taula de compliment de requeriments que s'inclou en aquest annex, degudament emplenada.

Aquesta taula té caràcter obligatori i permetrà comprovar, de manera clara i estructurada, que l'oferta presentada s'ajusta als requeriments tècnics, funcionals i de qualitat descrits en aquest plec.

El licitador haurà d'indicar, per a cada requisit:

- Compliment (Sí/No).
- Observacions o descripció del model proposat, si escau.

La manca de compliment d'algun dels requisits mínims establerts, o la falta d'informació suficient per verificar-lo, comportarà l'exclusió automàtica del licitador del procediment de contractació.

Així mateix, haurà de presentar-se, conjuntament amb aquesta taula, el full d'especificacions que permeti acreditar documentalment totes les característiques declarades.

Taula 1: Taula de compliment de requisits

Requisit	Descripció del requisit de la persona responsable del servei i interlocutora	Compliment (Sí/No)	Observacions
Lead auditor	Certificat com a *Lead auditor* qualificat, per una entitat certificadora		
Formació	L'auditor disposa d'un mínim de 40 hores de formació específica en la norma i esquema objecte de la contractació		
Experiència	Experiència com a auditor/a responsable o líder en tres (3) auditories de característiques similars a la present contractació, en els últims cinc (5) anys		

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://tramits.apdcat.cat/Ciutadania/ValidarDocuments.aspx?csv=b80fde1d-ca45-4f98-8e57-6f5840bf3e8c El destinatari del document ha de tractar el codi segur de verificació (CSV) que consta a l'encapçalament d'aquest document amb cautela, atès que la seva comunicació a terceres persones els permetria accedir al contingut del document.