

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS:

CONTRACTACIÓ DELS SERVEIS PER A REALITZAR UNA AUDITORIA INTERNA DEL SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ DE L'ORGANISME PAGADOR DELS FONS FEAGA-FEADER A CATALUNYA (UNE-ISO/IEC 27001) I DELS CONTROLS DE LA NORMA ISO/IEC 27002, PEL PERÍODE 2026-2028

1.- ANTECEDENTS:

El Reglament Delegat (UE) 2022/127, de 7 de Desembre, estableix en el punt 3.B) del seu annex I, on detalla els criteris d'autorització dels Organismes Pagadors dels fons FEAGA-FEADER (política agrària comunitària), els requeriments en relació amb la seguretat dels sistemes d'informació.

A Catalunya, el Departament d'Agricultura, Ramaderia, Pesca i Alimentació (DARPA) ha assumit la funció d'Organisme Pagador dels fons FEAGA i FEADER escollint i adequant la seguretat dels seus sistemes d'informació a la norma ISO/IEC 27002 (codi de bones pràctiques per a la gestió de la seguretat dels sistemes d'informació).

La norma certificable de la gestió de la seguretat dels sistemes d'informació és la norma ISO/IEC 27001. Per assolir aquesta certificació i maximitzar les garanties del compliment del requeriment davant de tercers, cal que anualment es duguin a terme auditories internes, les quals són l'objecte d'aquest contracte.

La Subdirecció General d'Auditoria i Inspecció Internes del DARPA és la unitat independent que té assignada la funció d'auditoria interna del DARPA.

2.- OBJECTE DEL CONTRACTE

L'objecte d'aquest contracte és l'assistència tècnica a la Subdirecció General d'Auditoria i Inspecció Internes del Departament d'Agricultura, Ramaderia, Pesca i Alimentació (DARPA) de la Generalitat de Catalunya en la realització d'una **auditoria interna del Sistema de gestió de**

la Seguretat de la Informació (SGSI) de l'Organisme Pagador dels fons FEAGA-LEADER de Catalunya segons la norma ISO/IEC 27001 i dels controls de la norma ISO/IEC 27002, durant el període 2026-2028.

3.- DESCRIPCIÓ DELS TREBALLS A REALITZAR

3.1. L'avaluació de la implementació efectiva de la Norma ISO/IEC 27001 en l'Organisme Pagador revisant:

- el sistema de gestió de la seguretat de la informació (SGSI) (punts del 4 al 10 de la norma) de manera anual en 2026, 2027 i 2028
- La revisió dels 93 controls de la Norma ISO/IEC 27002 (v. 2022) (recollits a l'annex A) al llarg del període 2026-2028

ISO 27002: 2022		2026	2027	2028
5.1	Polítiques per a la seguretat de la informació		X	
5.2	Rols i responsabilitats en seguretat de la informació		X	
5.3	Segregació de tasques		X	
5.4	Responsabilitats de la direcció			X
5.5	Contacte amb les autoritats		X	
5.6	Contacte amb grups d'interès especial		X	
5.7	Intel·ligència d'amenaçes	X		
5.8	Seguretat de la informació en la gestió de projectes	X		
5.9	Inventari d'informació i altres actius associats			X
5.10	Ús acceptable de la informació i actius associats			X
5.11	Devolució d'actius	X		
5.12	Classificació de la informació		X	
5.13	Etiquetatge de la informació	X		
5.14	Transferència de la informació	X		
5.15	Control d'accés	X		
5.16	Gestió d'identitat			X
5.17	Informació d'autenticació	X		
5.18	Drets d'accés			X
5.19	Seguretat de la informació en les relacions amb els proveïdors			X
5.20	Abordar la seguretat de la informació dins dels acords de proveïdors			X
5.21	Gestió de la seguretat de la informació en la cadena de subministrament de les TIC			X
5.22	Seguiment, revisió i gestió del canvi dels serveis de proveïdors	X		
5.23	Seguretat de la informació per a l'ús de serveis al núvol	X		
5.24	Planificació i preparació de la gestió d'incidents de seguretat d'informació			X
5.25	Avaluació i decisió sobre els esdeveniments de seguretat d'informació			X
5.26	Resposta a incidents de seguretat de la informació			X
5.27	Aprenent dels incidents de seguretat de la informació			X

ISO 27002: 2022		2026	2027	2028
5.28	Recopilació d' evidències			X
5.29	Seguretat de la informació durant la interrupció			X
5.30	Preparació per a les TIC per a la continuïtat del negoci			X
5.31	Identificació de requisits legals, reglamentaris i contractuals			X
5.32	Drets de propietat intel·lectual (DPI)			X
5.33	Protecció dels registres			X
5.34	Privacitat i protecció de dades de caràcter personal (DCP)			X
5.35	Revisió independent de la seguretat de la informació	X		
5.36	Compliment de les polítiques i normes de seguretat de la informació			X
5.37	Documentació de procediments operacionals		X	
6.1	Comprovació		X	
6.2	Termes i condicions de contractació		X	
6.3	Conscienciació, educació i formació en seguretat de la informació			X
6.4	Procés disciplinari			X
6.5	Responsabilitat davant la finalització o canvi			X
6.6	Acords de confidencialitat o no divulgació	X		
6.7	Teletreball		X	
6.8	Notificació dels esdeveniments de seguretat de la informació			X
7.1	Perímetre de seguretat física	X		
7.2	Controls físics d' entrada	X		
7.3	Seguretat d' oficines, despatxos i recursos	X		
7.4	Monitoratge de la seguretat física	X		
7.5	Protecció contra les amenaces físiques i ambientals		X	
7.6	El treball en àrees segures	X		
7.7	Lloc de treball enlairat i pantalla neta	X		
7.8	Emplaçament i protecció d' equips	X		
7.9	Seguretat dels equips fora de les instal·lacions	X		
7.10	Suports d' emmagatzematge	X		
7.11	Instal·lacions de subministrament		X	
7.12	Seguretat del cablejat		X	
7.13	Manteniment dels equips		X	
7.14	Eliminació o reutilització segura d' equips	X		
8.1	Dispositius finals d' usuari		X	
8.2	Gestió de privilegis d' accés			X
8.3	Restricció de l' accés a la informació		X	
8.4	Accés al codi font		X	
8.5	Autenticació segura		X	
8.6	Gestió de capacitats		X	
8.7	Controls contra el codi maliciós		X	
8.8	Gestió de vulnerabilitats tècniques		X	
8.9	Gestió de la configuració		X	
8.10	Eliminació de la informació		X	
8.11	Emmascarament de dades		X	
8.12	Prevenició de fuites de dades		X	

ISO 27002: 2022		2026	2027	2028
8.13	Còpies de seguretat de la informació		X	
8.14	Redundància recursos de tractament de la informació		X	
8.15	Registres d' esdeveniments		X	
8.16	Seguiment d' activitats		X	
8.17	Sincronització del rellotge		X	
8.18	Ús dels programes d' utilitat amb privilegis		X	
8.19	Instal·lació del programari en sistemes en producció	X		
8.20	Seguretat de xarxes			X
8.21	Seguretat dels serveis de xarxa			X
8.22	Segregació en xarxes			X
8.23	Filtratge de webs			X
8.24	Ús de la criptografia			X
8.25	Seguretat en el cicle de vida del desenvolupament	X		
8.26	Requisits de seguretat de les aplicacions	X		
8.27	Seguretat en el cicle de vida del desenvolupament	X		
8.28	Codificació segura	X		
8.29	Proves de seguretat en desenvolupament i acceptació	X		
8.30	Externalització del desenvolupament	X		
8.31	Separació dels entorns de desenvolupament, prova i producció	X		
8.32	Gestió de canvis	X		
8.33	Dades de prova	X		
8.34	Protecció dels sistemes d' informació durant les proves d' auditoria		X	
		31	32	30

93
CONTROLS

93

- Anualment s'hauria d'auditar la principal seu central del DARPA a la Gran Via de Barcelona, així com 2 de les seus en què actua l'Organisme Pagador ja sigui en alguna de les altres seus (no principals) del DARPA a Barcelona capital, com a les ubicades a la resta de Catalunya

Cal tenir present que l'abast tècnic del SGSI de l'Organisme Pagador està constituït per:

SEUS		Ubicació	Serveis Centrals	Serveis Territorials	Oficines Comarcals / Demarcació
3 seus (SSCC)	Seu 1 - BCN- Gran Via	BCN capital	SSCC		
	Seu 2 - BCN- Dr Roux	BCN capital	SSCC	ST Barcelona	Comarca del Barcelonès
	Seu 3 - BCN - districte administratiu de la zona franca	BCN capital	SSCC		
4 (demarcació de Barcelona)		Barcelona			Resta OC demarcació de Barcelona
7 Seus (demarcació de Girona)		Girona		ST Girona	Comarca del Gironès
		Demarcació de Girona			Resta OC demarcació de Girona
5 Seus (demarcació de la Catalunya Central)		Vic		ST Catalunya central	Comarca d'Osona
		Demarcació de la Catalunya Central			Resta OC demarcació de la Catalunya central

SEUS	Ubicació	Serveis Centrals	Serveis Territorials	Oficines Comarcals / Demarcació
7 Seus (demarcació de Lleida)	Lleida		ST Lleida	
	Demarcació de Lleida			Resta OC demarcació de Lleida
5 Seus (demarcació de Tarragona)	Tarragona		ST Tarragona	Comarca del Tarragonès
	Demarcació de Tarragona			Resta OC demarcació de Tarragona
4 Seus (demarcació de Terres de l'Ebre)	Terres de l'Ebre		ST Terres de l'Ebre	OC Baix Ebre
	Demarcació de Terres de l'Ebre			Resta OC demarcació de Terres de l'Ebre
7 Seus (demarcació de l'Alt Pirineu i Aran)	Alt Pirineu i Aran		ST Alt Pirineu i Aran	
	Demarcació de l'Alt Pirineu i Aran			Resta OC demarcació de l'Alt Pirineu i Aran
4 Seus (demarcació del Penedès)	Penedès		ST Penedès	OC de l'Alt Penedès
	Demarcació del Penedès			Resta OC demarcació del Penedès
TOTAL SEUS: 46				

3.2. S'haurà d'incloure també la revisió de l'estat d'implementació de les mesures pendents derivades d'auditories anteriors. La Subdirecció li facilitarà la descripció de les mesures pendents i l'adjudicatari haurà de verificar si han estat o no implementades.

3.3. La formulació de recomanacions i proposta d'un pla d'acció actualitzat acordat.

4.- PROGRAMA DE TREBALL

Un cop adjudicat el contracte, l'empresa adjudicatària elaborarà un programa de treball, detallant les proves a realitzar per a dur a terme aquest contracte, lliurant-lo a la Subdirecció en els primers 10 dies. Aquest programa (pla de proves) haurà de ser aprovat per la Subdirecció General d'Auditoria i Inspecció Internes del DARPA.

5.- CALENDARI D'EXECUCIÓ DELS TREBALLS:

Calendari 2026:

- Esborrany d'informe, papers de treball de suport i evidències **com a molt tard 15 de juny de 2026, 2 mesos després de la signatura del contracte (com a màxim el 15 d'abril**

del 2026) *(aquests documents hauran d'assolir la validació de la SBDGAI en un termini no superior a 5 dies hàbils des d'aquesta data).*

- Informe definitiu, papers de treball de suport, evidències i pla d'acció acordat amb els auditats **com a molt tard el 15 de juliol de 2026, 3 mesos després de la signatura del contracte.**

Calendari 2027-2028:

- Esborrany d'informe, papers de treball de suport i evidències **com a molt tard el 15 de juny de cada any** *(aquests documents hauran d'assolir la validació de la SBDGAI en un termini no superior a 5 dies hàbils des d'aquesta data).*
- Informe definitiu, papers de treball de suport, evidències i pla d'acció acordat amb els auditats **com a molt tard el 15 de juliol de cada any.**

6.- EXECUCIÓ DEL TREBALL, SUPERVISIÓ I LLIURAMENT DELS RESULTATS DEL TREBALL

Mentre duri l'execució del contracte, la Subdirecció General d'Auditoria i Inspecció Internes exercirà la supervisió dels treballs. Aquesta supervisió inclourà, a part de l'esmentada en relació amb el programa de treball, els papers de treball realitzats, l'informe que se'n derivi, així com el pla d'acció corresponent.

Periòdicament, la Subdirecció General d'Auditoria i Inspecció Internes requerirà a l'empresa adjudicatària informació sobre l'estat d'execució dels treballs i documentació de suport, amb l'objecte de poder efectuar el pertinent seguiment/supervisió dels mateixos.

Com a resultats del treball, l'empresa escollida haurà de lliurar:

- El PROGRAMA DE TREBALL esmentat (especificant l'abast, tipus de proves, dates previstes per les verificacions, auditor actuant, auditat-interlocutor).
- Els PAPERS DE TREBALL de suport de l'avaluació de cadascun dels punts de les normes revisades, així com les evidències. Aquesta documentació s'haurà de facilitar de manera clara i ordenada per tal de facilitar la seva revisió abans de l'emissió de l'esborrany d'informe.
- Un INFORME. Aquest haurà de ser en català (en suport digital) on es detallin:

- L'abast de les verificacions realitzades
 - La descripció dels fets observats (amb la referència (codi) dels papers de treball que suportin les anàlisis)
 - Conclusions
 - Recomanacions (detallant grau d'importància i dificultat per a la seva implementació).
- RESUM EXECUTIU, clar i sense terminologia tècnica, que permeti transmetre el resultat de l'auditoria d'una manera entenedora, no sols pels responsables de les TIC.
 - Un PLA D'ACCIÓ amb la concreció de les mesures correctores i terminis d'implementació acceptat per part dels responsables.

La SDGAI haurà de revisar els papers de treball i evidències lliurades i l'esborrany de l'informe, podent efectuar els comentaris / modificacions que consideri oportuns fins arribar a un acord en relació amb l'esborrany a lliurar. L'esborrany consensuat d'informe serà tramès als responsables dels sistemes d'informació de l'OP per tal que puguin fer les al·legacions que considerin oportunes en un termini de 10 dies hàbils. Un cop valorades aquestes al·legacions per part de l'empresa adjudicatària i comentada i acceptada la seva valoració amb la SDGAI, s'emetrà el corresponent informe definitiu.

L'informe serà assumit per la SDGAI en la mesura que s'ajusti al contingut del present plec de clàusules.

7.- PERSONAL QUE ES DESTINARÀ A L'EXECUCIÓ D'AQUEST CONTRACTE

El projecte requereix de la participació d'un:

- **Cap de projecte (a temps parcial)**: que dirigeixi a l'auditor, validi la planificació del projecte, supervisi el treball i coordini les reunions de seguiment.
 - Ha de disposar del CISA (Certified Information System Auditor)
- **Auditor de seguretat (a temps complet)**: serà qui realitzarà el treball de camp, obtindrà les evidències i revisarà els controls i mesures de seguretat adoptades.

- Ha de disposar del CISA (Certified Information System Auditor

L'adjudicatari haurà d'adscriure al projecte els professionals els currículums dels quals hagi presentat, llevat raons justificades cas en el qual haurà d'aportar professionals de qualificacions equivalents a les valorades en el procés de contractació.

8.- HORES MÍNIMES DE DEDICACIÓ DEL PROJECTE

El projecte no podrà tenir una dedicació d'hores inferior al 85% de **461,55h** (en total) considerades en els càlculs del Preu base de licitació (132,32h en 2026, 130h en 2027 i 130h en 2028).

9.- PROPIETATS DELS TREBALLS I CLÀUSULA DE CONFIDENCIALITAT

La documentació generada durant l'execució d'aquest contracte serà propietat exclusiva del DARPA, quedant dipositada a la Subdirecció General d'Auditoria i Inspecció Internes.

L'empresa adjudicatària haurà de mantenir reserva absoluta de la informació obtinguda en el desenvolupament d'aquest servei i no podrà utilitzar per a ell, ni proporcionar a tercers, cap dada del treball contractat, ni publicar totalment o parcial el contingut dels informes sense autorització escrita del DARPA. L'adjudicatari serà responsable dels danys i perjudicis que ocasioni.

Barcelona, a data de la signatura electrònica

Per delegació, la secretària general
(Resolució ACC/469/2022; DOGC 8616, 01.03.2022)

Cristina Massot Berna