



Contractació i Patrimoni

INFORME TÈCNIC

TITOL: EN RELACIÓ A L'ACORD, SI ESCAU, DE L'ADJUDICACIÓ DEL CONTRACTE DEL SERVEI DE DELEGAT/DA DE PROTECCIÓ DE DADES DE L'AJUNTAMENT DE VILANOVA I LA GELTRÚ I ELS SEUS ENS MUNICIPALS

En Jaume Meseguer Linares, en la seva condició de tècnic-lletrat de l'Ajuntament de Vilanova i la Geltrú, **INFORMA:**

Antecedents de Fet

I.- Primer.- La Secretaria General de l'Ajuntament de Vilanova i la Geltrú, ha emès informe justificatiu de necessitat de la contractació, les característiques i l'import del contracte de serveis de delegat de protecció de dades de l'Ajuntament de Vilanova i la Geltrú, d'acord amb l'article 28.1 i 116 de la LCSP i l'article 73 RGLCAP.

II.- Mitjançant Decret d'alcaldia nº 2424 de data 28 d'abril de 2021, es va resoldre incoar expedient del servei de delegat de Protecció de Dades de l'Ajuntament de Vilanova i la Geltrú i els seus ens dependents.

III.- Atès que la Junta de Govern Local de l'Ajuntament, en la sessió del dia 1 de juny de 2021, va adoptar per unanimitat l'acord següent:

“PRIMER. APROVAR l'expedient de contractació, l'obertura del procediment d'adjudicació mitjançant procediment obert simplificat, els plecs de clàusules tècniques i administratives particulars que s'incorporen respectivament com a Annex I i Annex II per a la contractació dels serveis de delegat de protecció de dades de l'Ajuntament de Vilanova i la Geltrú.

SEGON. CONVOCAR licitació per procediment obert simplificat, no subjecte a regulació harmonitzada i no és susceptible de recurs especial en matèria de contractació, d'acord amb els articles 145, 146, 159 i concordants de la LCSP, per un període de 2 anys, prorrogable 3 anys més per períodes anuals, i amb un pressupost base de licitació de 24.000 € més 5.040 € corresponents al 21% d'IVA, que fan un total de 29.040 € (VINT-I-NOU MIL QUARANTA EUROS), pel 2 any de durada del contracte.”

En data 2 de juny de 2021, es va dur a terme la publicació de l'anunci de licitació en el perfil del contractant.

III.- En data 30 de juny de 2021, el Servei de Contractació d'aquest Ajuntament es procedeix, en sessió telemàtica i en compliment d'allò que preveu els articles 140 i 326.2 a) de la LCSP i les clàusules 1.10), 1.11) i 1.12) del Plec de clàusules administratives particulars que regeix la contractació de referència, es procedeix a la constitució de la Mesa de Contractació, i a l'obertura i qualificació de la documentació del sobre B.



AJUNTAMENT DE
Vilanova i la Geltrú

Contractació i Patrimoni

Que les següents empreses han presentat memòria justificativa:

UNIVE ABOGADOS UNIÓN TEMPORAL DE EMPRESAS
SOTHIS SERVICIOS TENCNOLÓGICOS S.L.
SEGURDADES, SL
ECIX GROUP, SL
TECNOLAWYER
GLOBAL LEGAL DATA SL
OBJETIVO TARSYS SL
GOVERTIS ADVISORY SERVICES, S.L.

CRITERIS QUE DEPENEN D'UN JUDICI DE VALOR

D'acord amb la clàusula 1.12.1 del PCAP, s'estableixen els Criteris d'adjudicació que depenen d'un judici de valor es puntuaran fins a 20 punts.

Els licitadors hauran de presentar una proposta de memòria tècnica i organitzativa d'un màxim de 10 pàgines, a format del foli Dina 4, en relació a la qual es valoraran els aspectes que es relacionen a continuació, amb un màxim de 20 punts i d'acord amb els següents subcriteris:

1. Programa de formació i de sensibilització en matèria de protecció de dades. Màxim 10 punts:

Consisteix en presentar una proposta de formació sobre el RGPD i la Llei Orgànica 3/2018, de Protecció de dades, adreçada a l'Ajuntament de Vilanova i la Geltrú i el seu grup institucional, establint el nombre d'hores anuals, amb un calendari de sessions informatives i els àmbits concrets de la formació d'acord amb el PPT.

Es puntuarà en funció de les hores ofertes i de la detecció de necessitats de formació en l'àmbit d'aplicació del contracte determinat al PPTP i serà condició imprescindible per a poder obtenir puntuació en aquest criteri que la formació es pugui impartir mitjançant sistemes telemàtics mitjançant plataforma online.

2. Enfocament basat en el risc (auditories): assessorar, assumir la realització i supervisió d'auditories internes o la coordinació d'auditories externes, formació, determinar quins recursos es deuen destinar a quines operacions de tractament, etc. Màxim 10 punts:

L'empresa licitadora ha de presentar una proposta de realització de controls i d'auditoria regulars. Com a mínim durant el període de contracte s'haurà de portar a terme una auditoria en l'àmbit del tractament de dades, en les obligacions establertes a l'RGPD i la LOPDGDD per a l'Ajuntament i les seves entitats.

El contingut mínim de l'auditoria haurà de ser:

- Determinació del grau d'adequació i compliment respecte la normativa.
- Identificació de la situació actual de cada requeriment legal i - si s'escau - de les deficiències detectades.



Contractació i Patrimoni

- Mesures correctores o complementàries per corregir les mesures correctives.
- Evidències d'auditoria
- Conclusions de l'auditoria.

L'auditoria estarà adreçada a garantir-ne el compliment de l'Ajuntament han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com el risc per als drets i les llibertats de les persones i les característiques de les organitzacions.

El licitador haurà de presentar la proposta de controls i auditoria proposats. S'atorgarà major puntuació en funció dels controls regulars proposats (tipologia, número i periodicitat) i dels requisits següents referents: planificació, desenvolupament i gestió de l'auditoria, realització de reunions amb les àrees, eines tecnològiques i varietat de mecanismes de gestió i controls, supervisió i seguiment de les mesures correctives i així com les possibles millores que el licitador consideri adient proposar.

Pel que fa a la valoració i puntuació de les memòries tècniques justificatives presentades:

GOVERTIS ADVISORY SERVICES, S.L.

1) Formació i sensibilització en protecció de dades:

Govertis ofereix un Pla de Formació en Protecció de Dades per al personal de l'Ajuntament i els ens associats que es distribuirà segons el perfil dels assistents:

- Formació genèrica per al personal.
- Formació específica per a responsables d'unitats administratives, àrees, seccions o departaments.
- Formació específica per a personal d'Informàtica.
- Formació específica per a càrrecs electes.

Les sessions de formació s'oferiran a través d'una plataforma on-line que Govertis posa a disposició de l'Ajuntament. S'oferiran dues sessions anuals en directe de cadascuna de les quatre formacions. Les sessions online en directe es realitzaran en períodes semestrals.

Les sessions quedaran enregistrades en vídeo i disponibles per al seu visionat per part dels usuaris que no hagin pogut assistir a la sessió en directe.

En el següent gràfic es mostra el plantejament de planificació de les sessions de formació per a un període de 12 mesos **(20h en total de formació anuals)**:

Primer semestre (10h):

Usuaris	2h
Responsables	3h
Informàtica	3h
Càrrecs electes	2h



Contractació i Patrimoni

Segon semestre (10h):

Usuaris	2h
Responsables	3h
Informàtica	3h
Càrrecs electes	2h

L'empresa licitadora proposa un temari de planificació en formació de protecció de dades i com a complement al Pla de formació, s'ofereix un programa de conscienciació i sensibilització per promoure, de forma continuada, la cultura de la protecció de dades.

2. Enfocament basat en el risc (auditories):

L'empresa licitadora Govertis ofereix una auditoria diferenciant tres fases:

- Fase pre-auditoria
- Fase d'execució
- Fase de resultats

La fase de pre-auditoria és la fase inicial del procés i ha de servir per configurar què es vol revisar, qui realitzarà l'auditoria, quan, on i com. Per tant, en aquesta fase, l'equip auditor ha de determinar els següents punts:

- objectius de l'auditoria
- abast de la mateixa
- criteris o marcs de referència
- planificació de treballs a realitzar
- programa d'auditoria

La fase d'execució correspon al procés "pas a pas" de seguiment d'activitats planificades en la fase de pre-auditoria. L'execució segueix sempre una mateixa estructura, iniciant-se amb la reunió d'obertura, continuant amb el treball de camp i finalitzant amb la reunió de tancament i presentació de l'informe de conclusions d'auditoria. En aquesta fase, l'obtenció d'evidències és l'activitat més important del procés, i ha de proporcionar informació suficient i objectiva per permetre arribar a la fase de resultats i poder elaborar l'informe.

Per dur a terme la recopilació d'evidències i la verificació del compliment dels principis, **s'establirà un pla d'entrevistes amb els responsables de les següents àrees** (llista no exclusiva):

- Secretaria
- Arxiu
- Administració Electrònica i TIC
- Seguretat i Protecció Ciutadana / Policia Local
- Recursos Humans
- Educació / Escoles Municipals
- Serveis Socials / Acció Social / Dependència
- Oficina d'Atenció al Ciutadà (OAC)
- els ens municipals dins de l'abast del contracte



Contractació i Patrimoni

La fase de lliurament de resultats és la fase final i on l'auditor valora les evidències recollides durant el treball de camp. L'informe que genera l'auditor ha d'explicar quina és la seva valoració respecte de l'organització auditada i el nivell de compliment dels criteris d'auditoria. **L'informe d'auditoria inclourà:**

- Introducció a l'informe, incloent una declaració dels objectius, de l'abast, normativa analitzada, relació d'entrevistes, identificació d'activitats de tractament i una descripció de l'ens municipal auditat.
- Abast, Amb indicació de data i lloc, així com dels participants.
- Nomenclatura utilitzada en l'informe.
- Anàlisi diferencial del grau d'adequació i compliment respecte a la normativa.
- Qüestionari d'auditoria, on s'identifiqui la mesura a complir, l'estat actual de compliment per part de l'organització, les desviacions detectades que portaran aparellades accions de millora i les recomanacions. Es diferenciaran les mesures jurídiques de les tècniques.
- Resultat del grau d'adequació i compliment.
- Conclusió i opinió general de l'auditor respecte als objectius plantejats.

L'empresa Govertis, estableix el següents **objectius i controls a revisar en l'auditoria:**

Sistema de gestió de protecció de dades i seguretat
Tractament de dades
Principis relatius al tractament
Exercici de drets
Corresponsables i encarregats del tractament
Mesures de seguretat tècniques i organitzatives
Avaluacions d'impacte en la protecció de dades (EIPD)
Transferències internacionals de dades

L'auditoria inclourà un informe de situació en protecció de dades, en el qual s'analitzarà el nivell de maduresa en seguretat dels diferents controls en matèria de protecció de dades. L'informe permetrà conèixer el nivell de compliment de l'entitat amb referència a una escala de maduresa basada en CMM.

Planificació de l'auditoria: S'establirà una auditoria de protecció de dades amb periodicitat anual. El DPD serà l'encarregat d'establir les tasques de preparació a l'auditoria i de proposar a l'Ajuntament les dates de realització.

Preparació de l'auditoria: Tasques de supervisió del DPD; formació i conscienciació; implantació de mesures tècniques, jurídiques i organitzatives.

Auditoria:

15 dies abans	Presentació pla d'auditoria
7 dies abans	Confirmació calendari Identificació interlocutors
Dia 1	Presentació equip auditor Recopilació d'informació Inici de les entrevistes
Dia 2	Finalització entrevistes



Contractació i Patrimoni

	Revisió de mesures de seguretat Validació d'evidències
Dies 3 a 5	Elaboració de l'informe d'auditoria
7 dies després	Presentació informe auditoria Proposta de mesures correctives

ECIX:

1) Formació i sensibilització en protecció de dades:

Durant les fases inicials de la prestació del servei i del coneixement de l'Ajuntament, es determinarà el pla de formació més adequat per a cada àrea o departament de l'organització que ho necessiti.

Tanmateix, a partir de l'anàlisi inicial també es decidirà sobre la conveniència de realitzar formacions genèriques en matèria de protecció de dades. Durant la prestació del servei es poden detectar necessitats formatives específiques a partir, per exemple, de consultes recurrents, la incorrecta implementació d'un protocol/política interna.

Per tant, ECIX proposen dues tipologies de formació, en funció de la temàtica a tractar i del personal a la que van dirigides:

Formació genèrica: Aquesta formació es dirigeix a tot el personal de l'Ajuntament, per aquest motiu la temàtica és molt ampla i serveixen per assentar conceptes bàsics de la protecció de dades.

Formacions específiques: Aquestes formacions segueixen el format més clàssic de transmissió de coneixement (es a dir, de manera presencial o bé mitjançant mitjans telemàtics), amb la particularitat que les temàtiques són molt més concretes i, per tant, només es dirigeixen a aquell personal de àrees determinades de l'Ajuntament que, per les seves responsabilitats, tingui accés a dades personals i segons les necessitats detectades de conformitat amb allò establert al punt 2.1.1. anterior.

Proposen tant formació presencial com telemàtica. Disposen de l'eina TEAMS de Microsoft que permet la interacció directa amb els alumnes tant per mitjà audiovisual com per mitjà escrit. Aquesta també permet la gravació de les formacions, això permet que es puguin posar els vídeos a disposició dels assistents per poder-ho visionar més tard i així poder assimilar conceptes més complexos.

Previsió de formació: Presenta una proposta orientativa de un calendari de formació, amb contingut i identificació de àrees que, segons la nostra experiència, seria necessari aplicar a l'Ajuntament. Per poder fer arribar el coneixement sobre la normativa de protecció de dades als empleats i col·laboradors de l'Ajuntament, estimem que seran necessàries un estimat de **16h de formació anuals**, distribuïdes de conformitat amb la següent proposta.

Ofereixen formació genèrica per a tot l'Ajuntament i ens municipals.

Ofereixen formació específica per a cada àrea o departament (recursos humans, serveis socials, intervenció-tresoreria, comunicació, cultura, seguretat ciutadana etc.



Contractació i Patrimoni

2) Enfocament basat en el risc (auditories):

Controls i metodologia per a realitzar l'auditoria:

La metodologia seguida per realitzar l'auditoria de verificació del compliment de la normativa, implicarà revisar següents aspectes relacionats amb els tractaments de les dades de caràcter personal:

1. Inventari de Sistemes d'Informació, aplicacions amb dades personals i de tractaments (tècnic i organitzatiu)
2. Gestió de riscos i avaluacions d'impacte (legal, organitzatiu i tècnic)
3. Transparència, informació i consentiments (legal i tècnic)
4. Encarregats de tractament (legal, organitzatiu i tècnic)
5. Transferències internacionals de dades (legal)
6. Drets dels interessats (legal, organitzatiu i tècnic)
7. Gestió i notificació d'incidents de seguretat amb afectació a dades personals (tècnic)
8. Conservació i supressió de dades personals (organitzatiu i tècnic)
9. "Accountability" i responsabilitat proactiva (organitzatiu)
10. "Privacy by Design and by default" (legal, organitzatiu i tècnic)
11. Mesures de Seguretat (tècnic)

El procés d'auditoria es durà a terme en base a les següents activitats:

- Recull de tota la documentació rellevant en relació a la revisió de tots els aspectes descrits anteriorment.
- Reunions i entrevistes amb els responsables de cada àrea, o altres interlocutors que puguin aportar informació rellevant per a l'auditoria.
- Realització de proves o verificacions.
- Elaboració i lliurament de l'informe d'auditoria a l'interlocutor designat per l'Ajuntament, en el qual es descriuran:
 - Tots els treballs d'auditoria duts a terme
 - El detall de la informació, fets i observacions que constitueixin evidències de potencials deficiències de compliment
 - Les conclusions sobre el grau de compliment, juntament amb les recomanacions d'auditoria per corregir els potencials incompliments.

Proposta planificació i periodicitat de l'auditoria: Anual. Termini elaboració 10 setmanes (aproximat en funció de l'Ajuntament i necessitats detectades).

Desenvolupament i gestió de l'auditoria: El desenvolupament de l'auditoria seguirà tres fases amb l'objecte de recopilar informació de totes aquelles àrees auditades, revisar la documentació identificada i l'emissió del corresponent informe final d'auditoria.

Pel que refereix a l'apartat a) "**Elaboració del qüestionari de compliment normatiu**" s'elaborarà un qüestionari de compliment normatiu adaptat per a l'Ajuntament seguint les directrius marcades per les Autoritats de Control. Aquest qüestionari haurà de poder ser utilitzat tant per a revisar el nivell de compliment normatiu de l'Ajuntament en matèria de protecció de dades com per acreditar el nivell de compliment del principi d'"accountability".



Contractació i Patrimoni

Seguidament, a l'apartat b) **“Revisió de la documentació”** els objectius a seguir serà, un cop elaborat el qüestionari, mantenir entrevistes amb les diferents àrees objecte d'auditoria. Arrel d'aquestes reunions amb les diferents àrees, es revisaran totes aquelles evidències que s'hagin sol·licitat expressament i facilitades en el marc del qüestionari, amb la finalitat de verificar la seva existència. Aquesta revisió documental es realitzarà amb l'objectiu de detectar possibles riscos d'incompliment normatiu. Així mateix, es revisarà el repositori de documents per a tenir una llista de tota la documentació per a l'auditoria.

Per últim, l'apartat c) **“Emissió de l'informe”** indicar que s'emetrà, a la finalització de la auditoria, un **informe assenyalant les deficiències detectades** a i les mesures correctives proposades per tal de resoldre les incidències detectades.

En aquest sentit, **l'informe final d'auditoria tindrà el següent contingut mínim:**

- i. Determinació del grau d'adequació i compliment de la normativa.
- ii. Identificació de la situació actual de cada requeriment legal i, si escau, de les deficiències detectades.
- iii. Mesures correctores o complementàries per corregir les mesures correctives
- iv. Evidències d'auditoria
- v. Conclusions de l'auditoria

Mecanismes de control, gestió i supervisió i seguiment de mesures correctives: Arrel de les deficiències identificades en el desenvolupament de la tasca d'emissió de l'informe final d'auditoria, ECIX establirà un pla d'accions correctives identificant aquelles no conformitats i observacions detectades.

GLOBAL LEGAL DATA

1) Formació i sensibilització en protecció de dades:

GLOBAL LEGAL DATA proposa un programa de formació continuada dels treballadors municipals, mitjançant accions formatives que es realitzaran en tres capes o nivells:

a. Formació online per a tot el personal que siguin usuaris de dades personal. Aquesta formació dona cobertura en formació en matèria de protecció de dades a tot tipus de personal, usuari de tractament, garantint unes nocions bàsiques però suficients per reforçar la protecció de les dades personals a les que es pugui tenir accés.

b. Tallers/Temàtics referits a formació temàtica o per col·lectius determinats, com Contractació / Serveis Socials / Policia Local / OAC / Educació / Exercici de drets / Bretxes de seguretat/Avaluació d'impacte ...)

c. Píndoles formatives de debat, en format de sessions breus d'actualització de coneixements.

- Proposa un temari de programa de formació i tallers.



Contractació i Patrimoni

- A través de MYDPO (plataforma de gestió de compliment normatiu de la legislació sobre protecció de dades, que inclou formació online), titularitat de GLOBAL LEGAL DATA, s'ofereixen cursos generals de protecció de dades (bàsic i avançat), curs de DPD i curs sobre protecció de dades de salut.
- Ofereix un programa de formació online continuat pels dos anys de contracte amb diversos nivells (bàsic, avançat i personalitzat (policia local, serveis socials, salut, contractació etc) i amb una planificació trimestral.
- Número d'hores ofertes en concepte de **formació 53 hores anuals**, d'acord amb el següent quadre:

Formació online per a tot el personal	4 hores
(Curs bàsic)	
Formació online per a tot el personal	4 hores
(Curs avançat)	
Formació online de dades de salut	4 hores
Taller Temàtic sobre protocol	3 hores
d'exercici de drets	
Taller Temàtic sobre protocol de	3 hores
bretxes de seguretat	
Taller Temàtic sobre gestió d'	3 hores
avaluació d'impacte	
Taller Temàtic per a serveis socials	3 hores
Tallers Temàtics per a la Policia Local	6 hores
Tallers Temàtics per al personal de	3 hores
contractació	
Tallers Temàtics per al personal de	3 hores
l'OAC	
Tallers Temàtics per al personal des	3 hores
serveis d'educació	
Tallers Temàtics per al personal de	3 hores
Promoció Econòmica/Servei	
d'Ocupació	
Sessió directius / Càrrecs electes	3 hores
Sessions breus d'actualització /	8 hores
(Píndoles formatives online)	

Per tant, proposen un pla de formació trimestral anual de 53h (2 anys de contracte):

Formació (bàsica, avançat i personalitzat)= 12 hores anuals
Tallers temàtics= 30 hores anuals
Sessió directius/ càrrecs electes= 3 hores anuals
Píndoles informatives= 8 hores anuals.

2) Enfocament basat en el risc (auditories):

El DPD designat donarà suport a les tasques de realització d'auditories de compliment en matèria de protecció de dades i supervisarà els resultats, d'acord amb les següents funcions de (informació, assessorament, supervisió i verificació).

GLOBAL LEGAL DATA proposa la realització de d'una auditoria anual i controls periòdics en matèria de Protecció de Dades, d'acord amb les següents fases:



Contractació i Patrimoni

- Fase de preauditoria
- Fase d'execució
- Fase de lliurament de resultats

Així mateix, GLOBAL LEGAL DATA aplicarà la següent metodologia en la realització de l'Auditoria:

- Revisió i anàlisi de la documentació
- Comprovació de registres
- Entrevistes i qüestionaris
- reconeixement visual/treball de camp

Aspectes auditats:

1) Actuacions de comprovació relatives:

- Legitimació per al tractament de dades de caràcter personal
- Aplicació del Principis de Finalitat i Minimització de les dades personals.
- Inventari d'activitats de tractament
- Contractes amb proveïdors o empreses externes amb accés a les dades de caràcter personal.
- Contractes amb proveïdors o empreses externes sense accés a les dades de caràcter personal.
- Cessions / Canvis de Finalitat de dades personals, amb relació a altres administracions o entitats privades.
- Procediment per a l'atenció de l'exercici dels drets dels afectats (accés, rectificació, cancel·lació o oposició de dades).
- Polítiques de Privacitat
- Polítiques, normes i procediments relatius a les mesures de seguretat adoptades d'acord amb els riscos existents
- Mesures tècniques i organitzatives sobre normativa de protecció de dades en relació als llocs de treball i a les metodologies de treball

GLOBAL LEGAL DATA efectuarà controls trimestrals del grau de compliment de les obligacions previstes. L'objectiu principal consistirà en la revisió del compliment dels principis i drets de protecció de dades i de verificació del desenvolupament i de l'establiment de les mesures de seguretat de tipus tècnic, jurídic i organitzatiu requerides, així com en la realització d'altres actuacions complementàries.

Calendari elaboració auditoria:

- Fase preauditoria: 30 dies
- Fase d'execució: 15 dies + 7 dies (inspecció instal·lacions)
- Fase de lliurament de resultats:
 - 1) Elaboració i lliurament dels informes Preliminars: 7 dies
 - 2) Aportació d'observacions per l'Ajuntament: 7 dies
 - 3) Elaboració i lliurament dels Informes definitius: 7 dies
 - 4) Pla d'Acció (metodologia del Pla i d'execució de les solucions): 7 dies



Contractació i Patrimoni

SOTHIS

1) Formació i sensibilització en protecció de dades:

Per a dur a terme el correcte desenvolupament de la formació, Sothis, proposa una execució dividida en les fases que es mostren en la memòria aportada.

El Pla de formació s'oferirà en flexibilitat d'horaris per a adequar-lo de la millor manera possible als horaris del personal de l'Ajuntament.

Formació online mitjançant l'eina MSTEAMS.

Ofereix **tallers de formació:**

- Taller 1: Aspectes Bàsics Protecció de dades
- Taller 2: Aspectes Jurídics de Protecció de dades
- Taller 3: Sistema de Gestió de Protecció de dades
- Taller 4: Seguretat dels tractaments
- Taller 5: Decàleg de seguretat

La proposta de formació de Sothis, a validar a l'inici del servei és la següent:

Tipus activitat	Hores	Sessions	Total hores
Formació en línia	7	10	70
Píndoles bimensuals	0.15	12	3
Butlletins especialitzats	0.15	24	6
		Total	79 hores

Concretament pel que fa la **formació en línia** s'estableix els següents:

Aspectes bàsics protecció de dades	2h	Tots els empleats
Aspectes jurídics protecció de dades	1h	Personal jurídic
Sistema de gestió de protecció de dades	1h	Tots els empleats
Seguretat del tractament	2h	Tots els empleats
Decàleg de seguretat	1h	Tots els empleats
Total hores formació línia	7h	

El nombre de sessions de la formació en línia s'estableix en 10 sessions.

Pel que fa a les **píndoles bimensuals**, s'estableix un programa i es troben adreçades a tots els empleats, d'acord amb el detall establert en la memòria. Total hores 3h.

Pel que fa als **butlletins especialitzats** novetats i notícies relacionades amb (RGPD i LOPDGDD): 12 butlletins a l'any: 24 en total. Total hores 6h.



Contractació i Patrimoni

S'estableix una proposta de planificació del programa de formació durant els 2 anys de duració del contracte.

2) Enfocament basat en el risc (auditories):

Sothis inclou la realització d'una auditoria interna posterior per part d'un consultor de Sothis, independent a l'equip d'implantació seguint els principis rectors del procés d'Auditoria. Aquest consultor pertany al Pool d'experts i sense cost addicional per a l'Ajuntament.

Per la realització de l'auditoria s'estableixen en la memòria un seguit de condicions particulars que ha de complir l'auditor cap, que haurà de complir el següent:

- Experiència demostrable en l'àmbit de la seguretat de la informació.
- Posseir títol de Lead Auditor ISO 27001, CISA o similars.
- Certificacions tècniques i de gestió en seguretat de la informació.
- Experiència demostrable en ciberseguretat, gestió de riscos, models de control intern i seguretat tècnica.

La metodologia general que l'auditor aplicarà serà la següent:

- 1) Arrancada de l'auditoria: Presentació, planificació i calendari de treball.
- 2) Sol·licitud i revisió de la documentació RGPD/LOPDGDD:

- Política de privacitat.
- Registre d'activitats de Tractament.
- Anàlisi de necessitat de realitzar una anàlisi d'impacte.
- Anàlisi d'impacte.
- Procediment de bretxes de seguretat.
- Clàusules de contractes per a proveïdors, empleats, plecs, etc.
- Clàusules d'informació recollida de les dades i consentiment dels afectats.
- Moviment internacional de dades.

- 3) Auditoria in situ: Entrevistes amb el personal i d'observació. Revisar la categorització dels sistemes d'informació

Es realitzarà l'informe d'auditoria en el qual es reflectirà el grau d'adequació al RGPD.

Com a fruit del resultat de l'informe d'auditoria, es realitzarà una relació de Recomanacions, a manera de Pla d'Acció, orientades a esmenar les no conformitats detectades en el procés de revisió, juntament amb un calendari proposat de compliment d'aquestes Recomanacions, convenientment prioritzades.

El Pla d'Acció serà específic i detallat, identificant-se:



Contractació i Patrimoni

- El tractament afectat.
- El control normatiu compromès junt amb una avaluació del risc en el que s'incorre.
- L'acció correctora proposada, que haurà de ser específica i detallada, de manera que pugui ser abordada pels responsables de l'ajuntament.

L'informe d'auditoria proposat, estarà estructurat de la següent forma:

- *Objecte i abast d'auditoria*
- *Pla d'Auditoria*
- *Resum executiu:*
 - *Determinació del grau d'adequació i compliment respecte la normativa*
 - *Conclusions de l'auditoria*
- *Resum de troballes*
 - *Punts forts.*
 - *Oportunitats de millora.*
 - *No Conformitats.*
- *Pla de Millores*
- *Annex I: Nivell de maduresa*
- *Annex II: Equip auditor*
- *Annex III: Evidències d'auditoria*

TARSYS

1) Formació i sensibilització en protecció de dades:

Es proposa una formació adreçada a dos perfils:

- Personal de la corporació
- Caps de serveis

Es proposa un **pla de formació** dividit en dos apartats: **Formació general i una formació específica**. En la memòria proposa un temari tant per la formació general com per l'específica. Ambdues formacions es consensuaran amb l'Ajuntament. Així mateix s'acordarà amb l'Ajuntament el nombre de sessions i número de persones assistents.

Les **formacions** podran ser **presencials en les dependències municipals o telemàtiques**.

Al finalitzar el pla de formació, s'elaborarà per Tarsys un **informe resum amb les consultes realitzades** i posar a disposició una **àrea de Preguntes Freqüents**.

Ofereixen una **eina de d'avaluació online** per valorar l'efectivitat de les accions formatives.

Pel que fa a la **formació en línia**:

- Disposa d'un sistema propi de videoconferències.
- Disposa d'un mòdul de formació en línia. Té com objectiu oferir una formació continuada.



Contractació i Patrimoni

L'eina de formació permet la formació anònima o identificada amb materials estàtics i audiovisuals, permeten el seguiment dels alumnes/resultats:

- Data i hora de connexió dels usuaris.
- Temps dedicat a la formació total i per temari.
- Resultats de les avaluacions de validació de comprensió dels continguts.
- Consultes als consultors de Tarsys de dubtes dels continguts.
- Disposa de qüestionaris de coneixement en format test per cada subtema que compon cada mòdul.
- Servei de tutoria en línia: s'ofereix un dia per setmana en horari de matí durant la durada de la formació en línia un consultor de Tarsys estarà a disposició dels treballadors per resoldre telemàticament les qüestions relatives a la formació o el plantejament de situacions precises en les àrees.

Píndoles informatives: ofereix píndoles informatives de difusió formativa continuada.

Dedicació formació personal Tarsys: dedicació mínima 50h anuals.

2) Enfocament basat en el risc (auditories):

Tarsys ofereix l'elaboració d'auditories completes del compliment legal, controls de verificació regulars, avaluació continuada dels coneixements i necessitats del personal.

Es planifica l'auditoria de forma biennal.

Metodologia de l'auditoria:

- Revisió de la documentació existent
- Realització d'entrevistes amb un grup d'interlocutors
- Avaluació i revisió de la documentació utilitzada per al desenvolupament de les tasques diàries de l'Ajuntament.

Objecte de revisió en l'auditoria, d'acord amb els punts desenvolupats a la memòria tècnica justificativa presentada per Tarsys:

- Registre d'activitats de tractament.
- Mesures de seguretat.
- Política d'us dels mitjans i els recursos per part de les persones usuàries.
- Acord de confidencialitat amb les persones treballadores.
- protocol d'escletxes de seguretat.
- Clàusules en els plecs de licitacions i en els contractes amb clients i proveïdors.
- Contracte d'encarregat de tractament i cessió de dades.
- Exercici dels drets de les persones interessades.
- pàgina web.
- Sistemes de videovigilància.
- Compliment dels principis en la recollida i tractament de dades personals (licitud, limitació de finalitat, minimització, exactitud, limitació dels terminis de conservació).
- Obtenció dels consentiment en aquells àmbits on apliqui (difusió d'imatges, butlletins informatius...etc).



Contractació i Patrimoni

- Tractament de dades de categories especials (salut, ideologia, etc).
- Tractament de dades relatives a condemnes i infraccions penals.
- Aplicació dels principis de privacitat en el disseny i per defecte.
- Avaluacions d'impacte.
- Revisió de les funcions de DPD.
- Transferències de dades a països de tercers i organitzacions internacionals.
- Garantia de drets digitals.

Estructura de l'auditoria segons memòria tècnica justificativa:

- 1) Resum executiu.
- 2) Introducció.
- 3) Metodologia.
- 4) Àmbit i Abast de l'Auditoria.
- 5) Compliment de la normativa de protecció de dades i identificació de les deficiències, amb els següents punts d'anàlisi:
 - Aspecte auditat.
 - Indicador del nivell de compliment general.
 - Normativa aplicable (RGPD i LOPDGDD).
 - Situació actual.
 - Indicació de les evidències recollides.
 - Valoració de l'equip consultor.
 - Àmbit afectat.
 - Risc.
 - Accions correctives.
 - Accions de millora.
- 6) Conclusions generals de l'auditoria.
- 7) Aplicacions d'accions correctives per a la correcció de "no conformitats".
- 8) Definir les accions i tasques concretes per corregir les "no conformitats", tot consensuant amb l'ajuntament la prioritització de les accions a realitzar.
- 9) L'informe final de l'auditoria es presentarà i validarà davant la Comissió de Seguretat de l'Ajuntament.

Dins de les tasques d'auditoria, Tarsys proposa **controls regulars a fi d'avaluar el compliment**, d'acord amb els àmbits definits en la seva memòria. El seu objectiu serà l'actuació continua proactiva de verificació del compliment i porta un instrument de control complementari i coordinat amb les auditories periòdiques previstes.

Tarsys proposa un mínim de **14 controls anuals** (una mitjana de dos per entitat). Aquests punts de control es plantejaran i aprovaran prèviament en la Comissió de Seguretat.

Dins de l'àmbit de l'Auditoria i relacionat paral·lelament amb la formació de les persones empleades, Tarsys **proposa realitzar avaluació de coneixements**, qualitat del servei, mitjançant enquestes de nivell de coneixement del personal per determinar:

- Nivell de coneixement de la legislació i els procediments interns.
- Determinar les necessitats de formació i comunicació dels usuaris.
- Servir d'evidència en auditories i controls.



Contractació i Patrimoni

L'avaluació es portarà a terme amb l'eina de gestió pròpia de Tarsys amb una **periodicitat mínima de dues anuals per entitat, essent un total de 14 avaluacions de coneixements i necessitats.**

TECNOLAWYER

1) Formació i sensibilització en protecció de dades:

Realització d'un **pla de formació específic** per a cada Departament de l'Ajuntament així com per a cada Ens.

Es proposa la **realització de 25 hores anuals de formació** sobre Protecció de Dades i Llei de Transparència.

Destinataris del pla de formació:

- Tot el personal que tracti dades personals. Es faran sessions agrupades per departaments.
- Responsables de Protecció de Dades.
- Responsables de funcionament de la Plataforma.

El Pla de formació es podrà realitzar **presencial o en format webinar**.

Ofereix un **Dossier (format electrònic)** per el personal responsable i un altre, per l'usuari que ha de tractar dades personals.

Proposa un **Curs bàsic (online)**, de elaboració pròpia, sobre RGPD. Disponible a la plataforma de Formació online, equivalent a **3 hores de formació**.

- Permanentment actualitzat
- Accessible a tots els treballadors en qualsevol moment
- Certificat final d'aprofitament (superant test)
- Possibilitat de fer cursos a mida

La formació es podrà realitzar en sessió remota compartida (via Teams).

Informació continua:

- Novetats legislatives
- Nova Documentació
- Noves funcionalitats

2) Enfocament basat en el risc (auditories):

Tecnolawyer, proposa la realització d'una auditoria inicial (després amb caràcter anual) que compren l'Estructura Tècnic-Organitzativa, la Política de Informació, la Política de Seguretat i la Política de Infraestructures Tecnològiques i Organitzatives. A més, es revisen els punts següents:



Contractació i Patrimoni

- Supervisió del compliment, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa a les operacions de tractament i les auditories corresponents (veure apartat de Formació més endavant).
- Avaluació de la Anàlisi de Risc dels tractaments realitzats .
- Revisió del compliment dels principis relatius al tractament, com els de limitació de la finalitat, minimització o exactitud de les dades.
- Valoració de compatibilitat de finalitats distintes de les que varen originar la recollida inicial de les dades.
- Es disposa d'un assistent per realitzar verificacions periòdiques relatives al compliment de la normativa de protecció de dades.
- Es generen informes específics per al DPD.
- Supervisió del compliment en les pàgines web.

Execució de l'auditoria: Descobriment / Mapejat de dades | Tractaments | Bases de legitimació | Informació i Drets | Mesures de Seguretat / Organitzatives | Avaluació de Riscos. Informe d'Auditoria: valoració del nivell de compliment.

Revisió: Proposta de subsanació de totes les deficiències detectades en l'auditoria. Col·laboració amb l'equip de treball de l'Ajuntament per implementar les recomanacions recollides dins del Informe.

Millora: Recomanacions de millora respecte aquelles troballes que no arriben a constituir una "no conformitat".

UNIVE ABOGADOS

1) Formació i sensibilització en protecció de dades:

UNIVE, ofereix un pla de formació basat en dues accions concretes:

- Emissió mensual de notes de conscienciació (component jurídic i tècnic) per la seva distribució.
- Classes de formació presencial/online (**mínim 10 hores anuals**)
- La **formació anirà enfocada en els següents blocs:**
- **a) Conceptes bàsics:**
- **b) Adequació al RGPD dels tractament de dades de l'administració local.**
- **c) Funcions i obligacions del personal funcionari i el sector públic.**
- **d) Consultes freqüents**

2) Enfocament basat en el risc (auditories):

UNIVE disposa d'eines a fi de:

- realitzar anàlisis objectiu de riscos.
- Per a la realització de l'avaluació d'impacte.

UNIVE, realitzarà una avaluació inicial de l'estat de compliment de la normativa aplicable en matèria de protecció de dades mitjançant la anàlisi dels següents:

- RAT



Contractació i Patrimoni

- Anàlisi objectius dels riscos inherents a cadascun dels tractaments i la necessitat de dur a terme una avaluació d'impacte.
- Definició metodologia i realització avaluacions d'impacte en la protecció de dades personals.
- Mesures de seguretat aplicades en els tractament realitzats en suport paper i els seus controls periòdics.
- Elaboració, actualització i millora de clàusules informatives, consentiments informats, etc.
- Llistat de tercers proveïdors amb accés a dades personals i contractes d'encarregat de tractament amb cadascun d'ells. Procediment de contractació pública i models de plecs a fi d'analitzar el compliment dels requisits en matèria de protecció de dades.
- Llistat de tercers als quals es cedeixin dades personals i els corresponents acords de cessió de dades personals.
- Procediment atenció exercici de drets.
- Procediment de gestió i notificació de bretxes de seguretat
- Procediment de conservació i destrucció de dades personals i determinació dels mecanismes de destrucció segura.
- Procediment de privacitat des de el disseny i per defecte.
- Procediment anonimització de dades personals

Rere les conclusions realitzarà tasques d'adequació al RGPD (a desenvolupar durant el primer any de contracte).

Pla de l'Auditoria interna:

- 1) Planificació.**
- 2) Execució:**
 - Reunió inicial
 - Sol·licitud de documentació
 - Examen visual
- 3) Conclusions**

UNIVE, presentarà un **informe de l'auditoria** amb la següent estructura:

- Identificació de l'entitat auditada.
- Objectiu i abast de l'auditoria.
- Criteris en els quals es basa l'auditoria.
- Descripció de les mesures legals i organitzatives d'acord amb el RGPD.
- Revisió i comprovació de totes les mesures.
- Redacció de mesures correctores i complementaries.
- Conclusions de l'informe i propostes millores i esmenes.

UNIVE, proposa implantar un **Pla d'Acció**, amb el contingut i calendari establert en la seva memòria justificativa.



Contractació i Patrimoni

SEGURDADES

1) Formació i sensibilització en protecció de dades:

Segurdades ofereix un Pla de formació en format presencial i telemàtic utilitzant preferentment l'aplicació MS TEAMS.

El Pla de formació va adreçat a coordinadors d'àrea dels administradors de seguretat, el personal administratiu que consideri apropiat dels diferents departaments que fins ara no tenia formació en RGPD i LOPDGDD i es proposa la formació com indispensable:

- Departament de comunicació, ja que gestiona pàgines web i xarxes socials.
- Departament de RRHH i Departament de Jurídic
- Serveis socials
- Arxiu i OMAC
- POLICIA MUNICIPAL per a la idiosincràsia especial de les dades que accedeixen (sobre ensenya, Videovigilància i queixes) i la forma concreta del seu tractament.

Es proposa un pla de formació tota la plantilla de les mateixes en matèria de protecció de dades d'un **total de 20 hores**.

En base a la jerarquia de personal de les responsables s'establirà sessions formatives especialitzades per àrea i/o departament de manera que es pugui tractar de forma específica les especificitats del tractament de dades que poden afectar a cadascuna d'elles de la següent manera:

En aquest sobre no es revelaran dades relatives a les hores de formació:

1. Formació específica per al Departament de Comunicació
2. Serveis socials
3. Policia municipal
4. Arxiu i OMAC
5. Formació específica als Responsables de Seguretat per a tractar temes de videovigilància, dades de geolocalització, i l'ús de drons
6. Formació genèrica per a la resta d'usuaris de forma que es realitzaran sessions que siguin necessàries de forma telemàtica o online.

Es proposa l'elaboració d'una **guia formativa** exclusiva per als usuaris de la plantilla de les responsables del tractament, subdividit en tres blocs diferents:

- **Manual general**, per a la seva distribuir amb coneixements bàsics per a qualsevol usuari
- **Manual especial** per aquells usuaris que accedeixin a dades especialment protegides i, per tant d'una sensibilitat per rellevant.

Formació i material docent: La formació la impartirà sempre i, en tot cas, advocats especialistes en dret de les noves tecnologies i la privacitat. En el cas dels, administradors de seguretat, la part específica del curs la impartirà un enginyer informàtic o en Telecomunicacions.



Contractació i Patrimoni

Les presentacions es realitzaran amb suport d'una presentació en Power Point que es trobarà disponible per als participants de les sessions formatives.

Es posarà a disposició de les responsables del tractament de tot el material que necessitin en matèria de protecció de dades que les autoritats de control puguin elaborar per a garantir un millor compliment de la normativa

2) Enfocament basat en el risc (auditories):

Pla d'auditoria interna:

- Auditoria inicial:

Com a fase preliminar i la necessitat d'elaborar el mapa de tractaments o registre d'activitats de tractament. Aquesta és la primera part de les tasques que SEGURdades consultors realitzarà presencialment en els diferents espais. En aquest punt, s'examinarà els següents punts:

- Localització d'instal·lacions físiques, distribució i configuració física de sistemes informàtics. On es troba el servidor, el sistema de backup, la visibilitat de les pantalles dels usuaris per a una part de tercers.
- En el cas de disposar d'un sistema de videovigilància, es revisarà el sistema sobre el qual està configurat, les àrees de gravació, especialment si es tracta de públic o no.
- Revisió dels expedients o tractament registrats fins a la data, ja que segons la guia d'anàlisi de riscos de febrer 2018 publicat per l'AEPD aquest es el punt de partida per tenir registre d'activitats.
- Aplicacions que utilitzen per al tractament de dades personals i les finalitats per corroborar la legitimació dels mateixos.
- Relació d'usuaris que realitzen els diferents tractaments.
- Relació de tercers que accedeixen a dades personals, en la qualitat d'encarregats de tractament.
- Revisió de l'existència de polítiques BYOD per a l'ús de dispositius electrònics i plataformes que les responsables del tractament posa a disposició dels seus empleats.
- Anàlisi de les pàgines web propietat de les responsables del tractament i o gestionades per aquestes en els punts continguts a la memòria justificativa
- Anàlisi de les xarxes socials propietat de les responsables del tractament.
- Anàlisis de les aplicacions mòbils de les que es disposi.

A més de l'auditoria anual inicial, anualment, mentre que el contracte està vigent, en el **mes 12 de cada anualitat es realitzarà la fiscalització anual**, amb la finalitat de supervisar les no conformitats detectades en els anteriors, i detectar noves amenaces a resoldre.

El calendari ordinari d'execució dels treballs d'execució i lliurament dels **informes anuals d'auditoria serà de dos mesos** des de la visita i recollida de dades, d'acord amb el cronograma que s'estableix en la memòria justificativa.



Contractació i Patrimoni

Proposa oferir la PLATAFORMA Pilot RGPD®. El Pilot GDPR® a més de disposar de tota la documentació necessària en suport digital des d'un accés fàcil i segur, permet veure al Client, l'estat de les tasques i el punt en què es troba el projecte.

Per tant, i vist tot l'exposat anteriorment es **CONCLOU**:

Pel que fa als Pla de Formació continuada presentats per les empreses licitadores (màxim 10 punts):

Empresa	Hores anuals	Telemàtic/presencial	Millores	Puntuació
Govertis	20h	si	Formació general/específica – Plataforma online (dues sessions anuals–semestrals) – Material i vídeos formació disponibles al web – Proposta de temari – Butlletí informatiu seguretat i privacitat – Servei avisos/alertes	7 punts
Ecix	16h	si	Formació general/específica – proposta de temari – tests interactius a través de l'eina Kahoot – jocs de rols interactius	6'5 punts
Global	53h	si	– Formació general/específica – Plataforma online pròpia MYDPO – Tallers i píndoles informatives – presenta temari de formació (bàsic, avançat). Específic a través dels tallers i el curs de formació online planificació/programa – proves qüestionari test (online)	8,5 punts



Contractació i Patrimoni

			- Curs específic protecció dades salut.	
Sothis	79h	Si Formació online 7h 10 sessions (70h)	- Formació general/específica - Tallers de formació - Eina Kahoot - píndoles bimensuals - Butlletins mensuals - planificació/programa - Repositori documental	8 punts
Tarsys	50h (mínim)	Si - Sistema propi de videoconferències	- Formació general/específica - informe sobre consultes realitzades durant les formacions - àrea de preguntes freqüents (online) - Eina de d'avaluació online de la formació realitzada - mòdul de formació en línia (eina pròpia al web) - programa temari coneixements. - planificació/programa - Resultats de les avaluacions de validació de comprensió dels continguts. - qüestionaris de coneixement en format test per cada subtema que compon cada mòdul. - Servei de tutoria en línia - Píndoles informatives	8 punts
Tecnolawyer	25h	Si	- Formació general/específica - Dossier (format electrònic) - Curs bàsic propi	7 punts



Contractació i Patrimoni

			(online) - planificació/programa - Certificat final d'aprofitament (superant test) - Possibilitat de fer cursos a mida	
Unive	10h (mínim)	Si	- Formació general/específica - notes mensuals de conscienciació (component jurídic i tècnic) - planificació/programa - Apartat de preguntes freqüents. - Plataforma i vídeos de formació.	6 punts
Segurdades	20h	Si	- Formació general/específica - Formació específica als Responsables de Seguretat per a tractar temes de videovigilància, dades de geolocalització, i l'ús de drons - guia formativa (general/especifica)	5,5 punts

Totes les empreses ofereixen formació presencial/online, ja sigui mitjançant aplicacions com TEAMS o mitjançant eines pròpies. Pel que fa a les hores de formació anuals, sothis ofereix la millor proposta (79h) anual, però cal destacar també que l'empresa Tarsys estableix un nombre d'hores amb caràcter de mínim (50h), al igual que Unive (10h). Totes les empreses han ofert una formació tant específica (en atenció a les àrees: salut, atenció al ciutadà, RRHH, policia, etc) com general adreçada al personal de l'Ajuntament, càrrecs electes, amb temaris o programari detallat. Es valora positivament, fet que li atorga major puntuació, oferir tallers específics continuats, píndoles informatives, cursos online propis, butlletins mensuals a disposició d'aquest Ajuntament, com ofereixen per exemple Tarsys, Sothis, tecnolawyer i Global. Les empreses Global (8,5), Sothis (8) i Tarsys (8) obtenen la major puntuació en atenció tant al nombre d'hores ofertes, com per la qualitat i detall del pla o programa de formació tant general com específic (àrea de preguntes freqüents (online), eina d'avaluació online, mòdul de formació en línia (eina pròpia al web), resultats de les avaluacions de validació de comprensió dels continguts, qüestionaris de coneixement en format test per cada subtema que compon cada mòdul, Servei de tutoria en línia,



Contractació i Patrimoni

Píndoles informatives). Tot i que Sothis oferta un número major d'hores de formació online (10 sessions de 7h), considerem que l'oferta formativa (general i específica) de Global i Tarsys és més complerta.

Pel que fa a l'enfocament basat en el risc (auditories) Pla d'Auditoria (màxim 10 punts):

Totes les empreses licitadores han presentat la seva proposta d'auditoria amb un calendari o planificació, complint amb els següents:

- Determinació del grau d'adequació i compliment respecte la normativa.
- Identificació de la situació actual de cada requeriment legal i - si s'escau - de les deficiències detectades.
- Mesures correctores o complementàries per corregir les mesures correctives.
- Evidències d'auditoria
- Conclusions de l'auditoria.

Totes les empreses licitadores, presenten una proposta d'informe final amb determinació del grau d'adequació a la normativa, identificació de les incidències o aspectes a millorar detectats, i una proposta de resolució amb un pla d'aplicació de mesures correctives.

Pel que fa a la proposta de controls regulars i auditoria (tipologia, número i periodicitat) i dels requisits següents referents: planificació, desenvolupament i gestió de l'auditoria, realització de reunions amb les àrees, eines tecnològiques i varietat de mecanismes de gestió i controls, supervisió i seguiment de les mesures correctives, totes les empreses licitadores compleixen amb establir una auditoria basada en una planificació i amb un calendari de treball a fi de valorar mitjançant, entrevistes amb les diferents àrees, coneixement de l'entorn, revisió del RAT, tractament de dades (generals i especials), avaluació d'impacte, plantilles, contractes, etc.

L'empresa **Govertis**, estableix un ampli ventall amb objectius i controls a revisar en l'auditoria, sota diversos apartats (amb detall dels punts de verificació de cada apartat):

- Sistema de gestió de protecció de dades i seguretat:
 - a) Evidenciar l'existència d'un sistema per gestionar la protecció de dades d'acord amb el principi d'accountability (Responsabilitat proactiva) o, si no, proposar les mesures correctores oportunes.
 - b) Verificació del compliment de l'RGPD i la LOPDGDD: deure d'informació, consentiment, registre d'activitats de tractament, encarregats de tractament, exercici de drets ARSOPL, procediment de gestió i notificació de violacions de seguretat de les dades personals.
 - c) Verificació que hi hagi un procés d'apreciació de riscos que, amb independència de les possibles EIPD realitzades a determinats tractaments, tingui en compte com a mínim els riscos dels actius de l'organització relacionats amb, o que suportin o tractin, dades personals.
 - d) Verificació que hi hagi un sistema de seguiment d'accions de sistema de gestió (desviacions detectades en les auditories, accions de mitigació o tractament dels riscos apreciats, avaluació de les oportunitats de millora proposades, etc.).



Contractació i Patrimoni

e) Verificació del rol de DPD i altres definits en el sistema de gestió de la protecció de dades: obligatorietat, notificació i publicitat, designació i modalitat, funcions definides, etc.

- Tractament de dades:

a) Evidenciar el control de l'organització sobre els tractaments que impliquin operacions sobre dades personals, relacionats amb els tractaments de l'organització, o si no, proposar les mesures correctores oportunes.

b) Verificació del protocol d'identificació de nous tractaments i de comprovació dels existents.

c) Verificació del registre d'aquests i de la informació que es conserva.

d) Verificació de com s'avalua la idoneïtat de realitzar una EIPD.

e) Verificació que s'acrediti la licitud dels tractaments, ja sigui mitjançant consentiment, obligació legal, exercici de poders públics o interès legítim, segons el cas, conservant les evidències necessàries.

f) Verificació que s'identifiquin clarament aquells tractaments que operin amb categories especials de dades i existeixi legitimació per al seu tractament.

g) Verificació que s'identifiquin els tractaments que requereixen Transferències Internacionals de Dades (TID)

h) Verificació que s'identifiquin els tractaments que no requereixen identificació pel fet de demanar-se anònimament o per emprar tècniques d'anonimització.

i) Verificació que s'apliquin les mesures organitzatives i tècniques adequades en el disseny dels nous tractaments, amb vista a garantir la protecció de dades per defecte i des del disseny.

j) Verificar les possibles decisions individuals automatitzades, inclosa la possible elaboració de perfils.

- Principis relatius al tractament:

a) Evidenciar que el responsable del tractament és capaç de demostrar el compliment dels principis de protecció de dades atenent el principi d'accountability (responsabilitat proactiva), o si no, proposar les mesures correctores oportunes.

b) Verificació del principi de transparència en la recollida de dades personals: S'informa exhaustivament a l'interessat de la finalitat de la recollida de les dades, dels posteriors tractaments a què es veuran sotmesos i per part de qui i on (Art. 5.1.a) i (Art. 13 RGPD). Es distingeix quan les dades no hagin estat obtinguts directament de la persona interessada (art. 14 RGPD). Si és el cas, verificació de compliment del deure d'informació a les normatives locals de protecció de dades. Es verificarà el cicle de vida de les dades personals.

c) Verificació del principi de limitació de la finalitat en el tractament de dades personals: S'identifiquen els fins determinats, explícits i legítims dels tractaments.

d) Verificació del principi de minimització de dades en la recollida de dades personals: Aquestes són adequades, pertinents i limitades al que és necessari en relació amb les finalitats del tractament a què se sotmetran.

e) Verificació del principi d'exactitud de les dades: Es comprovarà l'existència d'un procediment que vetlli per aquesta exactitud, ja sigui de forma proactiva o fins i tot de forma reactiva davant l'exercici de drets per part dels interessats.

f) Verificació que es compleixi el principi de limitació en el termini de conservació: Es comprovarà que s'estableixi el termini de conservació de les dades de naturalesa personal i hi hagi procediments per garantir que es compleixen aquests terminis.



Contractació i Patrimoni

g) Verificació del principi de seguretat: Es verificarà a alt nivell que es disposa de mesures tècniques i organitzatives adequades per protegir les dades personals.

h) Verificació de compliment de les obligacions derivades de les normatives locals de protecció de dades.

i) Verificació que hi hagi rols i responsabilitats assignades en relació amb els procediments d'exercici de drets. Verificació que han rebut la formació adequada respecte al seu compliment o forma d'actuar.

j) Verificació dels canals de comunicació externa i interna. Verificar els formularis de resposta, si n'hi haguessin.

l) Verificació de si procedeixen limitacions a l'exercici de drets, en subjecció a mesures legislatives que emparin a determinats tractaments.

m) Verificació de compliment de les obligacions derivades de les normatives locals de protecció de dades.

- Exercici de drets:

a) Garantir, per part del responsable del tractament, l'exercici de drets dels interessats en forma i termini.

b) Verificació que hi hagi procediments definits pel que fa al dret d'accés (Art. 15 RGPD), rectificació (Art. 16 RGPD), supressió (Art. 17 RGPD), limitació del tractament (art. 18 RGPD) i, si escau, portabilitat de les dades (art. 20 RGPD) i oposició (Art. 21 RGPD). Comprovar que es tinguin en compte els terminis.

c) Verificació que hi hagi rols i responsabilitats assignades en relació amb els procediments d'exercici de drets. Verificació que han rebut la formació adequada respecte al seu compliment o forma d'actuar.

d) Verificació dels canals de comunicació externa i interna. Verificar els formularis de resposta, si n'hi haguessin.

e) Verificació de si procedeixen limitacions a l'exercici de drets, en subjecció a mesures legislatives que emparin a determinats tractaments.

f) Verificació de compliment de les obligacions derivades de les normatives locals de protecció de dades.

- Corresponsables i encarregats del tractament:

a) Assegurar les garanties suficients per als interessats pels tractaments de dades personals, amb independència de la cadena de tractament i/o de compartició de responsabilitat.

b) Verificació que s'hagin identificat els corresponsables dels tractaments.

c) Verificació que s'identifiquin els proveïdors, o terceres parts, determinant quins d'ells tracten o poden arribar a tenir accés a dades personals. (Art. 28 RGPD) i que hi ha un registre de tercers. Identificació d'aquells que requereixen d'una Transferència Internacional de Dades.

d) Verificació que s'hagin identificat els corresponsables dels tractaments, si fos el cas.

e) Verificació que s'acreditin en l'encarregat del tractament les garanties suficients per aplicar mesures tècniques i organitzatives apropiades -Diligència deguda (Art. 28.1 RGPD), o que s'acrediti l'adhesió de l'encarregat a un codi de conducta aprovat (Art. 28.5 RGPD) o a una certificació reconeguda.

f) Verificació que s'hagin subscrit els corresponents contractes o actes jurídics.

- Mesures de seguretat tècniques i organitzatives:

a) Garantir les mesures de seguretat tècniques i organitzatives, d'acord amb l'apreciació del risc, que garanteixin la seguretat de les dades personals i tractaments de dades de la institució.



Contractació i Patrimoni

b) Verificació de l'aplicació de mesures de seguretat tècniques i organitzatives adequades a l'avaluació del risc general de l'organització (Art. 32 RGPD) i específic dels tractaments (Art. 32.2 RGPD). Verificar com s'harmonitza amb les millors pràctiques de seguretat de la informació.

c) Verificació de la Declaració de Aplicabilitat, cas d'una organització obligada per les disposicions de l'ENS, respecte a com s'han implementat les mesures que es determinen en l'annex II d'RD 3/2010. Comprovar si s'han afegit mesures específiques per complir el RGPD en la referida Declaració de Aplicabilitat

d) Verificació, si escau, de la seudonimització i el xifrat de dades personals.

e) Verificació la capacitat de garantir les dimensions de la seguretat, inclosa la disponibilitat, dels sistemes de tractament i els serveis que aquests suporten, fins i tot davant un incident disruptiu.

f) Verificació, mitjançant mètriques i indicadors, de l'eficàcia de les mesures tècniques i organitzatives implantades per garantir la seguretat dels tractaments.

g) Verificació de l'existència d'un procediment per al tractament de violacions de seguretat de les dades personals, incloent la seva comunicació a l'autoritat de control i el seu registre.

h) Comprovació del mètode previst d'avaluació de risc que comporta la bretxa i la seva possible comunicació als afectats.

- Avaluacions d'impacte en la protecció de dades (EIPD):

a) Determinar l'impacte, dels tractaments d'alt risc, en els drets i llibertats dels interessats.

b) Verificació que es determina la idoneïtat de realitzar una EIPD per a tots els tractaments que, per la seva naturalesa, abast, context o finalitats, comportin un alt risc per als drets i llibertats de les persones físiques (art. 35.1 RGPD). Verificar el mètode de determinar la necessitat de realitzar aquesta EIPD.

c) Verificació, a partir del moment que es publiqui per part de l'autoritat de control, que es tenen en compte les llistes de tipus d'operacions de tractament que requereixin, o que no requereixin, EIPD.

d) Verificació del procediment de realitzar una EIPD, garantint que inclogui els aspectes que determina la norma.

e) Verificació dels registres de possibles EIPD realitzades i de les actuacions derivades dels possibles riscos inacceptables trobats.

f) Verificació dels criteris respecte a la posterior actualització de les possibles EIPD.

g) Verificació que en el procediment de realització de EIPD es tingui en compte els criteris i la informació necessària per elevar una consulta prèvia a l'autoritat de control.

- Transferències internacionals de dades:

a) Garantir que les possibles transferències internacionals de dades de la institució, ja sigui a tercers països o a organitzacions internacionals, compleixin les condicions establertes en RGPD.

b) Verificació que les TID basades en decisions d'adequació de la Comissió (garanties de nivell de protecció adequat).

c) Verificació de les TID que s'emparin en garanties adequades

d) Verificació, si escau, de les TID que es basin en normes corporatives vinculants.



Contractació i Patrimoni

e) Comprovació que hagin estat aprovades per l'autoritat de control (Art. 47 RGPD). Verificació que es compleixin en les TID les possibles condicions d'excepcionalitat.

ECIX proposa els següents objectius de control:

1. Inventari de Sistemes d'Informació, aplicacions amb dades personals i de tractaments (tècnic i organitzatiu):

- Identificació dels actius d'informació i dels controls implementats per garantir la confidencialitat, disponibilitat i integritat de les dades personals responsabilitat de l'Ajuntament.

- Revisió del registre d'activitats de tractaments: actualització i continguts mínims:

- Verificació de la existència de bases de licitud: revisió de que els tractaments tenen una base de licitud; revisió aleatòria de que les bases de licitud siguin adequades (màxim 5 tractaments)

2. Gestió de riscos i avaluacions d'impacte (legal, organitzatiu i tècnic):

Detecció de tractaments d'alt risc: es sol·licitarà documentació que acrediti que per tots els tractaments s'ha valorat si són d'alt risc, o no

- Comprovar l'existència d'una metodologia de gestió de riscos i/o avaluacions d'impacte (AIPD)

- Comprovar l'existència dels informes de riscos i de les AIPD realitzades: verificació que els riscos estan actualitzats: sol·licitud del darrer informe de riscos i de la darrera avaluació d'impacte (anàlisi continguts mínims i consistència)

- Comprovar l'existència d'un catàleg de controls legals, organitzatius i tecnològics per mitigar els riscos detectats

- Identificació de les mesures de seguretat implantades en funció del risc detectat en els tractaments: mapeig amb actius d'informació, tractaments i mesures (per a 3 tractaments)

3. Transparència, informació i consentiments (legal i tècnic):

Revisar model de clàusula informativa per a empleats: una mostra dels 5 últims contractes subscrits amb nous empleats.

- Revisar el model de clàusula informativa per a candidats.

- Revisió de la política de privacitat o de protecció de dades a la web, així com la política de "cookies".

- Comprovar l'existència d'un mecanisme d'obtenció, gestió i traçabilitat del consentiment, quan sigui aquesta la base legitimadora del tractament.

- Si és el cas, existència de l'avaluació que s'ha de dur a terme sobre l'interès legítim: per 1 tractament

- Revisió de la informació proporcionada en relació als sistemes de videovigilància i control d'accés.

4. Encarregats de tractament (legal, organitzatiu i tècnic):

- Revisió de l'inventari de proveïdors amb accés a dades personals.

- Verificar la disponibilitat d'una política i metodologia d'avaluació, selecció i gestió de proveïdors amb accés a dades personals.

- Control aleatori dels 3 últims contractes signats amb proveïdors que tinguin accés a dades personals responsabilitat de l'Ajuntament.

5. Transferències internacionals de dades (legal):



Contractació i Patrimoni

- Revisió de l'inventari de transferències internacionals de dades personals.
- Identificació si s'han previst garanties per cadascuna de les transferències internacionals.

6. Drets dels interessats (legal, organitzatiu i tècnic):

- Confirmar si s'ha posat a disposició dels interessats un canal de comunicació per a l'exercici dels seus drets i, si escau, identificació d'aquest canal i de com s'informa de la seva existència als interessats.
- Verificar l'existència d'un protocol intern d'atenció i resposta a l'exercici dels drets dels interessats.
- Si s'escau, confirmació de si s'han implementat mecanismes per atendre el dret a la portabilitat i identificació d'aquests mecanismes.
- Revisió del registre de les sol·licituds de drets rebudes.
- Revisió de les 3 darreres respostes donades com a conseqüència de les sol·licituds d'exercici de drets rebudes.

7. Gestió i notificació d'incidents de seguretat amb afectació a dades personals (tècnic):

- Verificar l'existència d'un procediment de gestió i notificació de les bretxes de seguretat a les autoritats de control, i en el seu cas de comunicació als interessats.
- Revisar el registre de les bretxes de seguretat que hagin pogut tenir lloc des de l'entrada en vigor de l'RGPD, com s'han gestionat, i les notificacions i comunicacions realitzades.

8. Conservació i supressió de dades personals (organitzatiu i tècnic):

- Revisió de la política de conservació de dades.
- Verificació de l'aplicació del procediments previstos.

9. "Accountability" i responsabilitat proactiva (organitzatiu):

- Confirmació de si s'han habilitat a la intranet o en un repositori accessible a tots els empleats totes les polítiques, protocols i procediments en matèria de protecció de dades.
- Si s'escau, verificació de si existeix un model de govern de la privacitat, i si s'estableixen rols i responsabilitats dins de l'entitat.
- Verificació de la designació del delegat de protecció de dades

10. "Privacy by Design and by default" (legal, organitzatiu i tècnic):

- Revisar l'existència d'una política interna que regula els procediments a seguir en les fases de disseny d'un servei que impliqui un tractament de dades personals que inclogui la revisió de el risc sobre la privacitat de l'afectat.

11. Mesures de Seguretat (tècnic):

- Revisió de l'avaluació de riscos tecnològics que determinin les mesures i controls de seguretat de les dades a implantar.
- Revisar el document en què es reculli en detall les mesures de seguretat aplicables al tractament de dades, a fi d'assegurar la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes que suporten els tractaments.
- Revisar el procediment de verificació, avaluació i valoració regular de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

En la proposta de ECIX, pel que fa a la revisió de diversos punts es troben limitats a un número concret de mostreig o revisió:

- Revisió aleatòria bases de llicitud (màxim 5 tractaments)



Contractació i Patrimoni

- identificació de les mesures de seguretat implantades en funció dels risc detectat en els tractaments: mapeig amb actius d'informació, tractaments i mesures (3 tractaments)
- revisió model clàusula informativa per a empleats: (una mostra dels 5 últims contractes subscrits amb nou empleats)
- Existència de l'avaluació que s'ha de dur a terme sobre l'interès legítim: (per 1 tractament)
- Control aleatori dels 3 últims contractes signats amb proveïdors que tinguin accés a dades personals responsabilitat de l'Ajuntament

GLOBAL proposa els següents objectius de control i que es detallen de forma amplia en la seva proposta en la memòria justificativa:

- Legitimació per al tractament de dades de caràcter personal
- Aplicació del Principis de Finalitat i Minimització de les dades personals.
- Inventari d'activitats de tractament
- Contractes amb proveïdors o empreses externes amb accés a les dades de caràcter personal.
- Contractes amb proveïdors o empreses externes sense accés a les dades de caràcter personal.
- Cessions / Canvis de Finalitat de dades personals, amb relació a altres administracions o entitats privades.
- Procediment per a l'atenció de l'exercici dels drets dels afectats (accés, rectificació, cancel·lació o oposició de dades).
- Polítiques de Privacitat
- Polítiques, normes i procediments relatius a les mesures de seguretat adoptades d'acord amb els riscos existents
- Mesures tècniques i organitzatives sobre normativa de protecció de dades en relació als llocs de treball i a les metodologies de treball

SOTHIS, inclou la realització d'una auditoria interna posterior per part d'un consultor de Sothis, independent a l'equip d'implantació seguint els principis rectors del procés d'Auditoria.

La metodologia general que l'auditor aplicarà serà la següent:

Sol·licitud i revisió de la documentació RGPD/LOPDGDD:

- Política de privacitat.
- Registre d'activitats de Tractament.
- Anàlisi de necessitat de realitzar una anàlisi d'impacte.
- Anàlisi d'impacte.
- Procediment de bretxes de seguretat.
- Clàusules de contractes per a proveïdors, empleats, plecs, etc.
- Clàusules d'informació recollida de les dades i consentiment dels afectats.
- Moviment internacional de dades.
- Entrevistes amb el personal i d'observació. Revisar la categorització dels sistemes d'informació.

En l'apartat 3.4 de la memòria justificativa es detalla els aspectes a auditar (a mode de resum):



Contractació i Patrimoni

- Principis relatius al tractament.
- Revisió de la licitud dels tractaments (base del consentiment, base legal).
- Revisió categories especials de dades personals.
- Revisió protocol actuació exercici de drets.
- Revisió dels contractes models de l'encarregat de tractament.
- Revisió del RAT
- Anàlisis del nivell de seguretat en la recollida i tractament de les dades.
- revisió del protocol de violacions de seguretat.
- Avaluació d'impacte i anàlisis de riscos.
- Revisió transferència internacional de dades.

TARSYS, proposa auditoria amb els següents objectes i àmbit de controls

- Revisió Registre d'activitats de tractament.
- Revisió de les Mesures de seguretat (suport informàtic, documental, seguretat física dels locals, còpies de seguretat, solucions informàtiques, control intern, gestió de la seguretat de la informació, etc).
- Política d'ús dels mitjans i els recursos per part de les persones usuàries.
- Acord de confidencialitat amb les persones treballadores (mecanismes de regulació del deure de confidencialitat i el seu coneixement per part del personal.
- protocol d'esclatxes de seguretat (coneixement del protocol, registre d'esclatxes de seguretat, etc).
- Clàusules en els plecs de licitacions i en els contractes amb clients i proveïdors. Contracte d'encarregat de tractament i cessió de dades. (tractament de dades realitzat per tercers, accions de control als encarregats de tractament, etc)
- Exercici dels drets de les persones interessades. (revisar protocol i avaluar el seu coneixement per part de l'ajuntament, revisió de la figura responsable, revisió de les sol·licituds, etc)
- pàgina web (enllaços i política de privacitat, avís legal, política de cookies).
- Sistemes de videovigilància (cartells informatius, ubicació, sistemes videovigilància etc).
- Compliment dels principis en la recollida i tractament de dades personals (licitud, limitació de finalitat, minimització, exactitud, limitació dels terminis de conservació).
- Obtenció dels consentiment en aquells àmbits on apliqui (difusió d'imatges, butlletins informatius...etc).
- Tractament de dades de categories especials (salut, ideologia, etc).
- Tractament de dades relatives a condemnes i infraccions penals.
- Aplicació dels principi de privacitat en el disseny i per defecte.
- Avaluacions d'impacte.
- Revisió de les funcions de DPD.
- Transferències de dades a països de tercers i organitzacions internacionals.
- Garantia de drets digitals (respecte dels drets dels treballadors a la protecció de la seva intimitat en l'ús dels dispositius digital professionals, revisió dret a la desconnexió digital, revisar la funció de control dels treballadors, revisió sistemes de geolocalització de treballadors).

Dins de les tasques d'auditoria, Tarsys proposa controls regulars a fi d'avaluar el compliment, d'acord amb els àmbits definits en al seva memòria. El seu objectiu serà l'actuació continua proactiva de verificació del compliment i porta un instrument de control complementari i coordinat amb les auditories periòdiques previstes.



Contractació i Patrimoni

Tarsys proposa un mínim de 14 controls anuals (una mitjana de dos per entitat). Aquests punts de control es plantejaran i aprovaran prèviament en la Comissió de Seguretat.

TECNOLAWYERS, proposa els següents objectius de control:

- Supervisió del compliment, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa a les operacions de tractament i les auditories corresponents (veure apartat de Formació més endavant).
- Avaluació de la Anàlisi de Risc dels tractaments realitzats .
- Revisió del compliment dels principis relatius al tractament, com els de limitació de la finalitat, minimització o exactitud de les dades.
- Valoració de compatibilitat de finalitats distintes de les que varen originar la recollida inicial de les dades.
- Es disposa d'un assistent per realitzar verificacions periòdiques relatives al compliment de la normativa de protecció de dades.
- Es generen informes específics per al DPD.
- Supervisió del compliment en les pàgines web.

Execució de l'auditoria: Descobriment / Mapejat de dades | Tractaments | Bases de legitimació | Informació i Drets | Mesures de Seguretat / Organitzatives | Avaluació de Riscos. Informe d'Auditoria: valoració del nivell de compliment.

UNIVE, proposa pel que fa a l'auditoria, els següents objectius de control i que es detallen de manera amplia en la seva memòria justificativa:

- Revisió del RAT
- Anàlisi objectius dels riscos inherents a cadascun dels tractaments i la necessitat de dur a terme una avaluació d'impacte (mitjançant eina pròpia).
- Definició metodologia i realització avaluacions d'impacte en la protecció de dades personals (mitjançant eina pròpia).
- Revisió Mesures de seguretat aplicades en els tractament realitzats en suport paper i els seus controls periòdics.
- Elaboració, actualització i millora de clàusules informatives, consentiments informats, etc.
- Llistat de tercers proveïdors amb accés a dades personals i contractes d'encarregat de tractament amb cadascun d'ells. Procediment de contractació pública i models de plecs a fi d'analitzar el compliment dels requisits en matèria de protecció de dades.
- Llistat de tercers als quals es cedeixin dades personals i els corresponents acords de cessió de dades personals.
- Procediment atenció exercici de drets.
- Procediment de gestió i notificació de bretxes de seguretat
- Procediment de conservació i destrucció de dades personals i determinació dels mecanismes de destrucció segura.
- Procediment de privacitat des de el disseny i per defecte.
- Procediment anonimització de dades personals

SEGURDADES, proposa la següent auditoria amb els objectius i controls que es detallen a la seva memòria justificativa:



Contractació i Patrimoni

- Localització d'instal·lacions físiques, distribució i configuració física de sistemes informàtics. On es troba el servidor, el sistema de backup, la visibilitat de les pantalles dels usuaris per a una part de tercers.
- En el cas de disposar d'un sistema de videovigilància, es revisarà el sistema sobre el qual està configurat, les àrees de gravació, especialment si es tracta de públic o no.
- Revisió dels expedients o tractament registrats fins a la data, ja que segons la guia d'anàlisi de riscos de febrer 2018 publicat per l'AEPD aquest es el punt de partida per tenir registre d'activitats.
- Aplicacions que utilitzen per al tractament de dades personals i les finalitats per corroborar la legitimació dels mateixos.
- Relació d'usuaris que realitzen els diferents tractaments.
- Relació de tercers que accedeixen a dades personals, en la qualitat d'encarregats de tractament.
- Revisió de l'existència de polítiques BYOD per a l'ús de dispositius electrònics i plataformes que les responsables del tractament posa a disposició dels seus empleats.
- Anàlisi de les pàgines web propietat de les responsables del tractament i o gestionades per aquestes en els punts continguts a la memòria justificativa
- Anàlisi de les xarxes socials propietat de les responsables del tractament.
- Anàlisis de les aplicacions mòbils de les que es disposi.

Eines de treball:

Empresa	Eines de treball
Govertis	Plataforma online
Ecix	Teams Microsoft
Global	Plataforma MYDPO
Sothis	- Teams Microsoft - Service Desk Plus
Tarsys	-Eina avaluació online -Plataforma online videoconferències - Teams Microsoft
Tecnolawyer	-Plataforma de Compliment Normatiu -Plataforma de Formació -Teams Microsoft -Plataforma de Helpdesk -Gestor documental i de projectes
Unive	-Plataforma de gestió -Plataforma de formació -Plataforma de contractes i documents legals OnLine
Segurdades	- Teams Microsoft - Plataforma Pilot RGPD®

Planificació i calendari, periodicitat controls:

Empresa	Planificació/calendari	Periodicitat	Controls
Govertis	Si	Anual	-
Ecix	Si	Anual	-



Contractació i Patrimoni

Global	Si	Anual	Trimestrals
Sothis	Si	Biennal	-
Tarsys	Si	Biennal	14 anuals
Tecnolawyer	Si	Anual	-
Unive	Si	Anual	-
Segurdades	Si	Anual	-

Les empreses Govertis, Ecix i Tarsys (per aquest ordre) ofereixen una proposta d'auditoria ampla i amb major grau de detall que els seus competidors. En el cas de Tarsys, ofereix la realització de 14 controls anuals. Per tot plegat, es proposa la següent puntuació:

Empresa	Puntuació auditoria
Govertis	8,5 punts
Ecix	7,5 punts
Global	7 punts
Sothis	7,5 punts
Tarsys	8 punts
Tecnolawyer	5,5 punts
Unive	6,5 punts
Segurdades	6 punts

Puntuació total criteris judici de valor:

Empresa	Puntuació formació	Puntuació auditoria	Total puntuació
Tarsys	8 punts	8 punts	16 punts
Govertis	7 punts	8,5 punts	15,5 punts
Global	8,5 punts	7 punts	15,5 punts
Sothis	8 punts	7,5 punts	15,5 punts
Ecix	6,5 punts	7,5 punts	14 punts
Tecnolawyer	7 punts	5,5 punts	12,5 punts
Unive	6 punts	6,5 punts	12,5 punts
Segurdades	5,5 punts	6 punts	11,5 punts.



AJUNTAMENT DE
Vilanova i la Geltrú

Contractació i Patrimoni