

Plantilla d'Avaluació d'Impacte relativa a la Protecció de Dades

Una avaluació d'impacte relativa a la protecció de dades (AIPD) és un procediment que busca identificar i controlar el riscs pels drets i les llibertats de les persones que resulten d'un tractament de dades personals.

Cal una descripció del tractament per determinar si es necessària una AIPD. Aquesta descripció ha de tenir un nivell de detall que permeti avaluar els supòsits i indicadors de risc que es detallen a continuació.

Descripció del tractament

--

No cal fer una AIPD si aplica algun dels supòsits següents:

Supòsit

El tractament té naturalesa, abast, context i finalitat semblant a un altre tractament pel qual ja s'ha fet una AIPD.	
El tractament té una base jurídica en el dret de la UE o d'un estat membre, i ja s'ha realitzat una AIPD en el moment d'adoptar aquesta base jurídica.	

Justificació

--

Si cap dels supòsits anteriors aplica, cal fer una AIPD si el tractament pot comportar un risc greu pels drets i les llibertats de les persones. El Grup de Treball de l'Article 29 (GT29) dona la següent llista de característiques que poden ser indicatives de risc alt.

Indicador de potencial risc alt

Avaluació o puntuació, incloses l'elaboració de perfils i prediccions.	
Presca de decisions automatitzada amb efectes jurídics o que afecta de manera similar i significativa a la persona física.	
Observació sistemàtica d'un àrea d'accés públic.	

Indicador de potencial risc alt

Dades sensibles, relatives a condemnes o infraccions penals, o dades que permetin determinar la situació financera.	
Dades biomètriques amb el propòsit d'identificar de manera única a una persona física.	
Dades genètiques per a qualsevol fi.	
Tractament de dades a gran escala.	
Conjunts de dades que s'han enllaçat o combinat.	
Dades relacionades amb persones vulnerables.	
Ús innovador de tecnologies.	
Tractament que en si mateix impedeix l'exercici d'un dret o l'ús d'un servei o contracte.	

Segons el GT29, cal fer una AIPD quan el tractament en presenta dues o més, tot i que indica que pot ser convenient fer l'AIPD fins i tot en alguns casos en què només en presenta una. Si n'hi ha dues o més i es considera que no cal fer una AIPD, cal justificar-ho.

Cal fer l'AIPD? Per què?

Si s'ha nomenat un DPD, cal considerar la seva opinió respecte de la necessitat de fer una AIPD.

Opinió del DPD respecte de la necessitat de fer una AIPD.

1. Descripció del Tractament

Cal fer una descripció del tractament que sigui el més detallada possible, ja que aquesta serà la base per avaluar la necessitat, la proporcionalitat i els riscos del tractament.

Descripció detallada del tractament

--

Finalitat del tractament

--

1.1 Dades personals tractades

Les característiques de les dades a tractar són rellevants a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del reglament.

Tipus de dada	
Font	
Termini de conservació	
Dada especialment sensible?	
Ús amb propòsit diferent al de recol·lecció?	

Tipus de dada	
Font	
Termini de conservació	
Dada especialment sensible?	
Ús amb propòsit diferent al de recol·lecció?	

1.2 Actors que intervenen en el tractament

Els actors que intervenen en el tractament, la seva funció i les dades que tracten són importants a l'hora de determinar els riscos del tractament.

Nom	
Processos en que intervé	
Descripció	

Nom	
Processos en que intervé	
Descripció	

1.3 Processos de tractament

L'objectiu d'aquesta secció és dividir el tractament en parts més petites. De manera que siguin més coherents i més fàcils d'explicar.

Procés	
Descripció	
Dades tractades	
Resultat del procés	
Persona destinatària	
Lloc del tractament	

Procés	
Descripció	
Dades tractades	
Resultat del procés	
Persona destinatària	
Lloc del tractament	

1.4 Transferències de Dades

Compartir dades amb agents externs pot incrementar els riscos del tractament; especialment si es fan a tercers països on l'RGPD no aplica.

Es comparteixen dades?

Descriu quines dades es comparteixen, la persona destinatària (física o jurídica) i la motiu/finalitat.

--

2. Necessitat i Proporcionalitat

L'avaluació de la necessitat i de la proporcionalitat del tractament es fa en relació a la finalitat del tractament, que s'ha descrit a la secció anterior.

2.1 Finalitat del tractament

En principi, les dades recollides s'utilitzen per assolir la finalitat del tractament que va motivar la recollida. Ara bé, en alguns casos, el Reglament permet el tractament de dades que han estat recollides amb una finalitat diferent.

S'utilitzen dades recollides amb una finalitat diferent a la d'aquest tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

En cas afirmatiu

Les següents condicions permeten el tractament de les dades amb una finalitat diferent a la de recollida.

S'ha obtingut el consentiment de les persones interessades pel tractament amb la nova finalitat.	
--	--

El tractament esta basat en el dret de la Unió o dels estats membres que constitueix una mesura per salvaguardar:

La seguretat nacional.	
------------------------	--

La defensa.	
-------------	--

La seguretat pública.	
-----------------------	--

Prevenció, investigació, detecció i el processament de delictes penals.	
---	--

Altres objectius importants d'interès públic.	
---	--

En cas afirmatiu

La protecció de la independència judicial i dels procediments judicials.	
La prevenció, la investigació, la detecció i el processament d'infraccions en normes deontològiques.	
La protecció de la persona interessada o dels drets i llibertats d'altres.	
L'execució de demandes civils.	

Si no aplica cap de les condicions anteriors, cal que la nova finalitat sigui compatible amb la finalitat que va motivar la recollida de les dades.

Finalitat inicial.	
Dades.	
Nova finalitat.	
Justificació de la compatibilitat.	
Finalitat inicial.	
Dades.	
Nova finalitat.	
Justificació de la compatibilitat.	

2.2 Principis de licitud i la lleialtat

2.2.1 Base legal pel tractament

Un tractament és lícit si aplica alguna de les bases legals següents:

La persona interessada ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	
El tractament és necessari per executar un contracte en què la persona interessada n'és part o per aplicar mesures precontractuals.	
El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.	
El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física.	

La persona interessada ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	
El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.	
El tractament és necessari per satisfer els interessos legítims del responsable del tractament o d'un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de la persona interessada (en particular, quan és un menor).	

Justificació de la licitud del tractament.

A banda, cal que el tractament no incorri en cap il·lícit en un sentit més ampli. Per exemple, infringir el copyright o acords contractuals.

Confirma que el tractament no incorre en cap tipus d'il·lícit.

2.2.2 Tractament de dades de menors

Els menors necessiten una protecció especial en el tractament de les seves dades, perquè poden no ser conscients dels riscos que comporta.

El tractament ofereix serveis de la societat de la informació a infants i té com a base el consentiment?	<input type="checkbox"/> Sí <input type="checkbox"/> No
En cas afirmatiu, s'ha tingut en compte l'edat mínima de consentiment?	<input type="checkbox"/> Sí <input type="checkbox"/> No

2.2.3 Tractament de categories especials de dades

Es tracten dades de categories especials?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

En cas afirmatiu

El tractament de categories especials de dades està prohibit, llevat que apliqui algun dels supòsits següents.	
La persona interessada ha donat el seu consentiment explícit per al tractament amb una finalitat específica, tret que el dret de la UE o de l'estat membre no ho permeti.	
El tractament és necessari per complir obligacions o per exercir drets en l'àmbit del dret laboral i de la seguretat i la protecció social.	
El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física, en el supòsit que l'interessat no estigui capacitat per donar el consentiment.	
El tractament és legítim i amb garanties, fet per una associació sense ànim de lucre de caràcter polític, filosòfic, religiós o sindical, sempre que el tractament afecti persones amb qui mantenen contactes en relació amb aquestes finalitats i les dades no es comuniquin a tercers sense el consentiment de les persones interessades.	
El tractament fa referència a dades que l'interessat ha fet manifestament públiques.	
El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.	
El tractament és necessari per raons d'interès públic essencial.	
El tractament és necessari per a finalitats de medicina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social.	
El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.	
El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.	

Justificació de la licitud del tractament de dades de categories especials.

2.2.4 Tractament de dades penals

Es tracten dades relatives a condemnes o infraccions penals?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

En cas afirmatiu

Tot i que les dades relatives a condemnes o infraccions penals no són categories especials de dades, hi ha un requisit addicional per tractar-les: el tractament només és pot portar a terme sota la supervisió de les autoritats públiques o quan ho autoritzi el dret de la unió o de l'estat membre.

Justificació de la licitud del tractament de dades penals.

--

2.2.5 Validesa del consentiment

Si un tractament té com a base legal el consentiment, cal que es compleixin les següents condicions perquè aquest sigui vàlid:

El responsable ha de poder demostrar que l'ha recollit.	
La sol·licitud de consentiment és intel·ligible, de fàcil accés i en un llenguatge clar.	
L'execució d'un contracte no es pot supeditar a rebre el consentiment respecte de dades personals no necessàries per executar el contracte.	
S'ha informat les persones interessades de la possibilitat de retirar el consentiment en qualsevol moment.	

2.2.6 Transferències de dades

Per evitar que les persones interessades vegin reduïts els seus drets, el RGPD és especialment restrictiu amb les transferències de dades amb països on el RGPD no aplica.

Es fan transferències a tercers països o a organitzacions internacionals?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

En cas afirmatiu

Aquestes transferències estan permeses si la Comissió Europea considera que el país o organització ofereix un nivell adequat de protecció, si s'han establert les garanties suficients segons l'article 46 o si aplica alguna de les excepcions de l'article 49.

Dades transferides.	
País.	
Condicció que permet la transferència.	

Dades transferides.	
País.	
Condicció que permet la transferència.	

2.2.7 Lleialtat del tractament

Un tractament és lleial si fa un ús de les dades previsible per part de les persones interessades, i del tractament no se'n deriven conseqüències adverses per a les persones interessades que no siguin justificables.

Justificació de tractament lleial.

--

2.3 Principi de minimització

Les dades han de ser adequades, rellevants i limitades a l'estrictament necessari per acomplir la finalitat del tractament.

Tipus de dades.	
-----------------	--

Justificació de l'adequació, la rellevància i la necessitat.

--

Tipus de dades.	
-----------------	--

Justificació de l'adequació, la rellevància i la necessitat.

--

Tipus de dades.	
-----------------	--

2.4 Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament. A la descripció del tractament, es va especificar el termini de conservació de les dades. Cal justificar que els terminis donats compleixen el principi de limitació del termini de conservació.

Justificació que els terminis de conservació donats compleixen amb la limitació del termini de conservació.

Cal que els mecanismes establerts per esborrar les dades siguin efectius (és automàtic o s'ha d'activar manualment? romanen les dades a les còpies de seguretat del sistema un cop esborrades? quant de temps i com es garanteix que no es tracten?)

Descriu els mecanismes establerts per esborrar les dades.

Les dades es poden conservar indefinidament amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.

Es conserven dades amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.	
---	--

En cas afirmatiu, quines mesures s'han implantat per garantir el principi de minimització.

2.5 Principi d'exactitud

El tractament de dades inexactes pot afectar negativament les persones. El principi d'exactitud demana que les dades siguin exactes i que es prenguin les mesures adequades per garantir que les que siguin inexactes s'actualitzin o s'esborrin sense dilació.

Controls de la qualitat de les dades.

Mesures per corregir les dades.

2.6 Riscos per les persones

L'objectiu d'aquest punt és identificar els possibles efectes negatius sobre les persones, quantificar-los i si és necessari proposar mesures per mitigar-los.

En aquesta secció avaluarem el tractament tal i com està dissenyat. És a dir, no considerem els casos en que falla la seguretat del sistema (sigui aquesta fallada accidental o intencionada).

En la identificació dels potencials efectes negatius del tractament sobre les persones convé tenir en compte el punt de vista de les persones interessades i del delegat de protecció de dades.

Potencials efectes negatius del tractament sobre les persones.

Per cadascun dels efectes negatius identificats, cal estimar el nivell de risc associat. El risc depèn de dos factors: l'impacte que té sobre les persones (baix, mitjà, alt o molt alt) i la probabilitat que es materialitzi (baixa, mitjana, alta). L'impacte s'estima directament dels potencials efectes. Per determinar la probabilitat, cal analitzar en quines circumstàncies fan que els efectes negatius és materialitzin (les amenaces) i estimar la probabilitat d'aquestes.

El risc es determina, en funció de l'impacte i de la probabilitat, seguint la taula següent:

Impacte				
Probabilitat	Baix	Mitjà	Alt	Molt alt
Alta	Risc mitjà	Risc alt	Risc alt	Risc alt
Mitjana	Risc baix	Risc mitjà	Risc alt	Risc alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc alt

Primer s'estimarà el risc associat a cada amenaça. El risc global serà el màxim dels riscos de les amenaces.

Efecte sobre les persones:

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat:

Efecte sobre les persones:

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat:

Llevat que el risc sigui baix, cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt o molt alt. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar l'autoritat de protecció de dades competent sobre la idoneïtat del tractament.

En cas que s'hagi alterat el tractament inicial per fer-lo menys lesiu per les persones, caldrà revisar i actualitzar les seccions anteriors de l'AIPD.

2.7 Necessitat i proporcionalitat del tractament

Amb la informació recollida en aquesta secció, cal justificar que el tractament és necessari (propòsit buscat no es pot atènyer amb cap altre mesura més moderada) i proporcional (no provoca més danys que beneficis).

Justificació de la idoneïtat del tractament pel propòsit que és busca.

Justificació de la necessitat del tractament.

Justificació que el tractament és proporcional.

2.8 Opinió de les persones interessades

L'RGPD estableix que, si és possible, cal recollir l'opinió de les persones interessades sobre el tractament.

Opinió les persones interessades sobre la necessitat i la proporcionalitat del tractament.

En cas que no es considera apropiat recollir l'opinió de les persones interessades, cal justificar-ho.

Per què no s'ha recollit l'opinió de les persones interessades?

Si l'opinió de les persones interessades respecte al tractament difereix de la visió que el responsable ha donat a l'apartat 2.7 i es pretén portar endavant el tractament, cal justificar el perquè.

Per què es porta endavant el tractament tot i les discrepàncies de les persones interessades?

3. Controls per Garantir els Drets de les Persones

3.1 Controls pel dret a tenir informació transparent

La transparència és transversal i ha de ser present en totes les comunicacions amb les persones interessades.

Tota comunicació amb les persones interessades ha de ser concisa, intel·ligible, de fàcil accés i ha de fer ús d'un llenguatge clar i senzill.	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

El reglament regula com s'ha de fer aquesta comunicació.

La informació es donarà per escrit (incloent mitjans electrònics).	<input type="checkbox"/> Sí <input type="checkbox"/> No
Pel cas de peticions fetes amb mitjans electrònics, la informació es donarà preferentment de forma electrònica.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si la persona interessada ho demana, la informació es donarà oralment.	<input type="checkbox"/> Sí <input type="checkbox"/> No

El responsable ha de respondre les peticions d'exercici de drets d'una persona interessada dins uns terminis establerts:

Sense demora indeguda i no més enllà d'un mes.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si la complexitat o el número de peticions ho justifica, es pot estendre el període en dos mesos. En aquest cas cal informar de les raons dins el primer mes.	<input type="checkbox"/> Sí <input type="checkbox"/> No

Si el responsable no ha de respondre a la petició d'exercici de drets d'una persona interessada, cal:

Avisar la persona interessada d'aquest fet sense demora indeguda i com a màxim en un mes.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Explicar les raons per no portar a terme la petició (per exemple, la petició és repetitiva o el responsable no pot identificar la persona interessada).	<input type="checkbox"/> Sí <input type="checkbox"/> No
Informar de la possibilitat de recórrer la decisió davant una autoritat supervisora o un jutjat.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Només si la petició és excessiva (per exemple, per repetitiva), es podrà cobrar un càrrec per cobrir els costos de tramitar-la.	<input type="checkbox"/> Sí <input type="checkbox"/> No

3.2 Controls pel dret d'informació

A l'hora de recollir dades personals, el responsable del tractament ha d'informar les persones interessades de diferents aspectes del tractament.

Els articles 13 i 14, especifiquen que cal informar les persones interessades dels punts a la taula següent:

La identitat i les dades de contacte del responsable.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Les dades de contacte del delegat de protecció de dades (si n'hi ha).	<input type="checkbox"/> Sí <input type="checkbox"/> No
La finalitat del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
La base legal del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'interès legítim del responsable, si aquesta és la base legal del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Els destinataris o categories de destinataris de les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El termini de conservació de les dades o el criteri emprat per determinar-lo.	<input type="checkbox"/> Sí <input type="checkbox"/> No
La intenció de transmetre les dades fora de la UE, si escau.	<input type="checkbox"/> Sí <input type="checkbox"/> No
La decisió de la Comissió Europea respecte de la suficiència de la seguretat que ofereix el país o organització destinatària.	<input type="checkbox"/> Sí <input type="checkbox"/> No

La identitat i les dades de contacte del responsable.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret d'accés a les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret de rectificació i supressió.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret de limitació del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret d'oposició al tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret de portabilitat de dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret a revocar el consentiment (si aquesta és la base legal del tractament).	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència del dret a presentar una reclamació davant una autoritat de control.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Que la comunicació de les dades és un requisit legal o contractual, si escau.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència de decisions automatitzades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El propòsit de fer servir dades amb una finalitat diferent a la que va motivar la recollida, si s'escau.	<input type="checkbox"/> Sí <input type="checkbox"/> No
La procedència de les dades, si no s'han obtingut directament de la persona interessada.	<input type="checkbox"/> Sí <input type="checkbox"/> No

Hi ha algunes exempcions a l'obligatorietat d'informar, que depenen de la forma en que s'han recollit les dades.

- Si les dades s'han obtingut directament de la persona interessada, no hi ha l'obligació d'informar-la si ja disposa de la informació.
- Si les dades no s'han obtingut directament de la persona interessada, no cal informar-la si es dona alguna de les següents condicions: la persona interessada ja disposa d'aquesta informació, la comunicació és impossible o suposa un esforç desproporcionat, així està regulat per una norma de la UE o dels estats membres o la informació té caràcter confidencial sobre la base del secret professional.

Si no s'informa, cal justificar-ho.

S'aplica el dret d'informació a totes les dades tractades?	
--	--

Si aplica alguna exempció al dret d'informació, cal dir quina, a quines dades i justificar el perquè.

S'aplica el dret d'informació a totes les dades tractades?	

Si s'informa les persones interessades, el Reglament determina quan cal fer-ho ¹.

Si les dades es recullen directament de les persones interessades, en el moment de recollir-les.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si les dades es recullen indirectament, cal complir les condicions següents:	
En un període raonable de temps i no superior a un mes.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si ens comuniquem amb les persones interessades, com a molt tard en el moment de la primera comunicació.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si es volen comunicar les dades a tercers, abans de comunicar-les.	<input type="checkbox"/> Sí <input type="checkbox"/> No

3.3 Controls per garantir el dret d'accés

La persona interessada té el dret d'obtenir del responsable del tractament la confirmació que s'estan tractant les seves dades i, en aquest cas, el dret d'accés a les dades personals i a la informació següent:

La finalitat del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Les categories de dades tractades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Les persones destinatàries de les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El termini de conservació de les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Els drets a rectificar i suprimir les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Els drets a limitar i oposar-se al tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El dret a reclamar davant una autoritat de control.	<input type="checkbox"/> Sí <input type="checkbox"/> No

¹ GDPR art 13(1) i 14(3),

La finalitat del tractament.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Si les dades no s'han obtingut de la persona interessada, l'origen de les dades.	<input type="checkbox"/> Sí <input type="checkbox"/> No
L'existència de decisions automatitzades, si escau.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Garanties en la transferència de dades fora de la UE, si escau.	<input type="checkbox"/> Sí <input type="checkbox"/> No

A banda de conèixer quina informació s'ha de transmetre a les persones interessades, cal assegurar-se que es donen les condicions per fer efectiu el dret d'accés.

S'ha establert un procediment estàndard per la gestió de sol·licituds d'accés?	<input type="checkbox"/> Sí <input type="checkbox"/> No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'accés?	<input type="checkbox"/> Sí <input type="checkbox"/> No

3.4 Controls per garantir el dret de rectificació

Les persones tenen el dret a que és rectifiquin les seves dades, si aquestes no són exactes.

S'ha establert un procediment per la gestió de sol·licituds de rectificació?	<input type="checkbox"/> Sí <input type="checkbox"/> No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de rectificació?	<input type="checkbox"/> Sí <input type="checkbox"/> No

Si el responsable ha compartit les dades, cal que informi les persones destinatàries sobre la rectificació.

S'ha establert un procediment per notificar la rectificació a les persones destinatàries?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

3.5 Dret de supressió

Les persones tenen el dret a que s'esborri la seva informació quan es dona algun dels següents casos:

- Les dades ja no són necessàries en relació amb la finalitat per què es van recollir.
- La persona interessada treu el seu consentiment i no hi ha cap altra base legal pel tractament.

- La persona interessada s'oposa al tractament i no hi ha cap altre factor superior que el legítim.
- Les dades s'han tractat sense una base legal.
- Les dades s'han d'esborrar d'acord amb una obligació legal que afecta el responsable.
- Les dades s'utilitzen per oferir serveis de la societat de la informació a infants.

En canvi, el dret de supressió no aplica en els següents casos:

- Per exercir el dret a la llibertat d'expressió i d'informació.
- Per complir una obligació legal o en l'interès públic.
- Amb la finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, i amb finalitat estadística (si el compliment d'aquestes finalitats es veïés afectat per la supressió de les dades).
- Per presentar, exercir o defensar reclamacions legals.

El personal té capacitat per decidir si aplica el dret a supressió?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

Es recomanable establir un canal estàndard perquè les persones interessades puguin demanar de fer efectiu el dret de supressió. Ara bé, cal assegurar-se que el personal està capacitat per detectar les sol·licituds que es facin per altres mitjans.

S'ha establert un procediment per la gestió de sol·licituds de supressió?	<input type="checkbox"/> Sí <input type="checkbox"/> No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de supressió?	<input type="checkbox"/> Sí <input type="checkbox"/> No

Si el responsable del tractament comparteix les dades, ha de prendre les mesures apropiades (tenint en compte els costos i la tecnologia disponible) per notificar les persones destinatàries sobre la petició de supressió.

S'ha establert un procediment per notificar la petició de supressió a les persones destinatàries?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

3.6 Dret a limitar el tractament

L'article 18 dona a les persones el dret a limitar el tractament de les seves dades, en els casos següents:

- La persona interessada ha demanat la rectificació de les seves dades i el responsable està verificant si són exactes.
- Les dades s'han tractat sense una base legal.
- La persona interessada necessita que el responsable guardi les dades per iniciar, exercir o defensar una reclamació.
- La persona interessada s'ha oposat al tractament i el responsable està avaluant si els motius legítims del responsable prevalen sobre els de la persona interessada.

El personal està capacitat per decidir si aplica el dret a limitar el tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds de limitació del tractament.

S'ha establert un procediment per la gestió de sol·licituds de limitació del tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de limitació del tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

A l'hora de limitar el tractament, cal tenir en compte les diferents formes que aquest pot tenir: recollida de dades, anàlisi de dades, disseminació de resultats, etc.

Es tenen en compte totes les possibles formes de tractament a l'hora de limitar-lo?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

Si s'han compartit dades, cal informar les persones destinatàries de les peticions de limitació del tractament.

S'ha establert un procediment per notificar la petició de limitació del tractament a les persones destinatàries?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

3.7 Dret a la portabilitat de les dades

Les persones tenen el dret a demanar les dades que han facilitat al responsable del tractament en els següents cassos:

- Si el tractament està basat en el consentiment, o és necessari per executar un contracte o per aplicar mesures precontractuals.
- El tractament es fa amb mitjans automatitzats.

El dret a la portabilitat de dades no es limita a les dades que les persones han donat de forma explícita; també afecta les dades que s'han recollit de l'observació de les persones.

El personal està capacitat per decidir si aplica el dret a la portabilitat de dades?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

El dret a la portabilitat de dades no ha d'afectar negativament a altres persones. En particular:

- Si les dades personals contenen informació d'una tercera persona, cal avaluar si aquesta darrera pot veure afectats els seus drets i llibertats.
- Si les dades estan associades a diverses persones (per exemple, un compte bancari compartit), cal buscar el consens de totes les persones interessades.

El procediment per fer efectiu el dret a la portabilitat de dades té en compte l'efecte sobre els drets i les llibertats de les altres persones?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

Cal assegurar-se que el personal està capacitats per detectar les sol·licituds de portabilitat de dades.

S'ha establert un procediment per la gestió de sol·licituds de portabilitat de dades?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de portabilitat de dades?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

El reglament determina la forma en la que s'ha de fer la portabilitat.

S'usa un format estructurat, d'ús comú i que sigui de fàcil lectura mecànica?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

3.8 Dret d'oposició

Les persones tenen el dret a oposar-se al tractament de la seva informació quan aquest tractament es fa sobre la base de:

- L'interès públic o l'exercici de poders públics conferits al responsable del tractament.
- L'interès legítim del responsable del tractament.

En aquest cas, el responsable ha de cessar en el tractament, llevat que acrediti motius legítims que prevalguin sobre els drets de l'interessat.

El personal està capacitats per decidir si aplica el dret a d'oposició?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

Cal assegurar-se que el personal està capacitats per detectar les sol·licituds d'oposició.

S'ha establert un procediment per la gestió de sol·licituds d'oposició al tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'oposició al tractament?	<input type="checkbox"/> Sí <input type="checkbox"/> No
--	---

El reglament especifica com s'ha d'actuar en rebre una petició d'oposició al tractament en diversos casos.

Si la petició s'oposa al tractament amb finalitats de màrqueting, aquesta ha de ser acceptada sense excepció.	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

Si la petició s'oposa al tractament amb finalitat d'investigació científica o històrica, o amb finalitat estadística, ha de ser acceptada llevat que el tractament es faci en l'interès públic.	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

3.9 Dret a no ser objecte de decisions automatitzades

Es fa un tractament automatitzat que té efectes jurídics o altres efectes significatius per les persones?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

En cas afirmatiu, quina base legal que ho permet?

És necessari per l'execució d'un contracte entre la persona interessada i el responsable.	
Està autoritzat pel dret de la unió o d'un estat membre.	
La persona interessada ha donat el seu consentiment explícit.	

La persona interessada sempre té dret a obtenir intervenció humana, a expressar el seu punt de vista i a impugnar la decisió.

Existeix un procediment perquè les persones puguin demanar intervenció humana, expressar el seu punt de vista i impugnar la decisió?	<input type="checkbox"/> Sí <input type="checkbox"/> No
Hi ha personal a l'organització amb la capacitat de revisar les decisions i canviar-les?	<input type="checkbox"/> Sí <input type="checkbox"/> No

Les decisions automatitzades només poden fer ús de categories especials de dades si hi ha el consentiment explícit de la persona interessada, o si el tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.

Es fa ús de categories especials de dades en el tractament automàtic?	<input type="checkbox"/> Sí <input type="checkbox"/> No
---	---

En cas afirmatiu, quina base legal que ho permet?

La persona interessada ha donat el seu consentiment explícit.	
El tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.	

4. Riscos en la seguretat de les dades

D'acord amb l'RGPD, les mesures emprades per protegir la informació han de ser apropiades al risc per als drets i les llibertats de les persones. En aquesta secció seguim una metodologia senzilla per analitzar els riscos relacionats amb la seguretat de les dades. És a dir, els riscos associats a la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades.

4.1 Impacte

Avaluem l'impacte que la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades personal tenen sobre la persona interessada.

Per fixar l'impacte sobre les persones de la pèrdua de la seguretat de les dades, cal tenir en compte les característiques del tractament. Entre d'altres:

- El tractament dades de categories especials o altres dades especialment sensibles (informació financera, localitzacions, etc.).
- La monitorització de persones.
- El tractament de dades de grups amb necessitats especials (menors, autoritats, etc.).
- El tractament de gran quantitat de dades de cada persona.

Amb l'objectiu de contextualitzar el càlcul de l'impacte, es plantegen diferents d'escenaris en que es perd alguna d'aquestes propietats.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones.

Exemples de casos de pèrdua de confidencialitat:

- Pèrdua o robatori d'un ordinador que conté dades personals.
- Enviament per error de dades personals a persones no autoritzades.
- Possibilitat d'accedir de forma no autoritzada al compte d'una persona.
- Un error de configuració en una web exposa les dades personals de les seves persones usuàries.
- Robatori d'informació de les instal·lacions del responsable o de l'encarregat del tractament.
- Un empleat d'un centre mèdic consulta de forma no autoritzada l'expedient d'un pacient.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones.

- Un empleat o empleada modifica per error les dades d'un client.
- Un error en la xarxa de comunicacions altera les dades mentre estan en trànsit.

- Per motius operacionals, una empresa manté diverses còpies de les dades, però un canvi en alguna de les còpies no és propaga a les altres.
- Pèrdua de part d'un expedient, com a conseqüència d'una fallada en el sistema de tractament.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.

Exemples de casos de pèrdua de la disponibilitat:

- Un fitxer és corromp o s'esborra i no hi ha una còpia de seguretat.
- Es perd un expedient del qual només hi havia una còpia en paper.
- Un servei de consulta de dades deixa d'estar disponible (per exemple, el servei per accedir al registres electrònics de salut).

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

L'impacte del sistema serà el màxim dels tres.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

4.2 Probabilitat inicial

La taula següent mostra característiques del tractament que incrementen els riscos de seguretat de les dades. Estimarem la probabilitat de fallada en la seguretat en funció del número de característiques es compleixen.

Maquinari i programari

Q1. El sistema de tractament està connectat a sistemes externs a l'organització?

La connexió amb sistemes externs a l'organització incrementa l'exposició a amenaces, podent la informació ser capturada o modificada maliciosament mentre està en trànsit. Això es produeix, per exemple, quan s'han contractat serveis al núvol, es realitzen connexions en modalitat de teletreball als sistemes de l'organització o es permeten accessos a través d'internet a la xarxa interna per connectar-se a les bases de dades corporatives, entre d'altres supòsits.

Sí No

Q2. Alguna part del tractament es fa a través d'internet?

La interacció amb les persones interessades a través d'internet exposa el sistema de tractament a amenaces externes, com ara *phishing*, *SQL injection*, *man-in-the-middle attacks*, *DoS* i *XSS*. Aquestes amenaces poden comprometre el sistema de tractament i afectar les propietats de seguretat de les dades (confidencialitat, integritat i disponibilitat).

Permetre que el personal accedeixi al sistema de tractament a través d'internet també incrementa l'exposició a atacs externs i, a banda, incrementa la possibilitat que el personal faci un mal ús de la informació (accidental o intencionat).

Alguns exemples d'aquests tipus de tractament poden ser els tractaments que fan ús del correu electrònic, aquells en què el manteniment o la supervisió es fa a través d'internet o bé l'ús de serveis al núvol com ara Google Drive, Microsoft One Drive, Amazon Web Services (AWS), Microsoft Azure, entre d'altres.

Sí No

Maquinari i programari

Q3. Manca document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?

Sí No

Si el sistema de tractament no està ben dissenyat o els elements que el componen no estan configurats adequadament els riscos per a la seguretat de les dades s'incrementen. Per garantir un bon disseny i una bona configuració del sistema de tractament hi ha multitud de guies en seguretat amb diferent temàtica que es poden adoptar per seguir-les, com ara de disseny de la xarxa local, tallafocs, segmentació de xarxa, xarxes privades virtuals (VPN), configuració de sistema operatiu, antivirus, ús de contrasenyes segures, múltiple factor d'autenticació (MFA), etc.

Disposar d'un document de bones pràctiques ajuda a dimensionar el sistema de tractament tenint en compte les necessitats computacionals, de comunicació, de seguretat i d'emmagatzematge. També permet configurar correctament el programari, aplicar una metodologia de desenvolupament que prioritzi la seguretat de les dades durant tot el cicle de vida de l'aplicació, utilitzar aplicacions segures en el núvol o establir criteris sobre l'ús i la tipologia de dades que es poden gestionar en aquest entorn, entre d'altres actuacions.

Q4. Manca document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?

Sí No

Disposar d'un document de bones pràctiques que reculli aquests aspectes és essencial per garantir el manteniment, la monitorització i un pla de resposta a incidents del sistema adequats. El manteniment s'ha de fer tant dels dispositius i maquinari com del programari. La monitorització permet analitzar un incident un cop s'ha produït i ajuda a detectar comportaments sospitosos a fi d'evitar que l'incident tingui lloc, o per reduir-ne l'impacte. El pla de resposta a incidents permet tenir un enfocament sistemàtic per abordar i gestionar els incidents de seguretat.

Aquest document de bones pràctiques pot recollir tasques importants com l'aplicació d'actualitzacions de seguretat del sistema operatiu, la realització de còpies de seguretat regulars, l'ús de sistemes automàtics de detecció o correlació d'esdeveniments de seguretat, així com la realització periòdica d'auditories per a la revisió de vulnerabilitats i la seguretat general, entre d'altres.

Q5. Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?

Sí No

La seguretat física de les instal·lacions de tractament és essencial. Sense això, no es pot garantir la seguretat del sistema de tractament (ja sigui electrònic o no). Això pot donar-se, per exemple, quan el CPD no està degudament protegit amb un sistema que impedeixi l'accés a les persones no autoritzades o no està protegit contra accidents naturals i industrials (fallades elèctriques, inundacions, etc.), quan l'arxiu s'ha distribuït en diferents àrees de manera que no se'n pugui garantir la seguretat o quan es fa un ús de serveis al núvol sense tenir garanties que les instal·lacions del proveïdor estan degudament protegides, entre d'altres supòsits.

Ús del sistema de tractament

Q6. Hi ha una manca de claredat en la definició dels rols i les responsabilitats del personal?

Sí No

Una manca de claredat en la definició dels rols i les responsabilitats pot donar lloc a un ús descontrolat de les dades (ja sigui accidental o intencionat). Per exemple, un treballador només hauria de consultar les dades que li són necessàries per dur a terme les seves tasques. També ha de ser responsable de destruir la informació quan ja no sigui necessària, així com de garantir-ne la seguretat quan es comunica a una altra organització o persona, entre d'altres.

Q7. Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?

Sí No

Quan els usos acceptables dels sistemes de tractament no estan definits clarament, s'incrementa el risc de fer-ne un mal ús i d'introduir vulnerabilitats al sistema. Per exemple, la instal·lació d'un programari de compartició de fitxers podria comportar la compartició involuntària d'informació o accedir a pàgines web malicioses podria facilitar l'entrada de programari maliciós i de robatori de dades, entre d'altres riscos.

Q8. Pot el personal connectar dispositius externs al sistema?

Sí No

La connexió de dispositius externs (telèfon mòbil, memòria USB, etc.) al sistema de tractament pot representar un risc de seguretat, atès que pot facilitar l'entrada de programari maliciós, la introducció de vulnerabilitats i l'extracció no autoritzada d'informació. Per aquest motiu, és imprescindible establir una política clara que reguli l'ús de dispositius externs per part del personal de l'organització.

Q9. Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?

Sí No

La manca d'un registre de les activitats (log file) pot afavorir les males pràctiques del personal i dificultar la investigació d'incidents un cop s'han produït, atesa la manca de traçabilitat, tal com estableix l'Esquema Nacional de Seguretat (ENS). Aquest fet compromet la capacitat de detectar, analitzar i respondre a possibles amenaces. Per tant, és necessari disposar d'un registre adequat que permeti conèixer qui accedeix als sistemes d'informació i assegurar que les activitats registrades siguin monitoritzades de manera efectiva.

Persones que intervenen en el tractament

Q10. El personal rep permisos que no són necessaris per complir les tasques que té encomanades?

Sí No

Com més gran sigui el nombre de persones que tenen accés a unes dades, més gran és la probabilitat que es produeixi un abús. Per evitar-ho, és essencial que el sistema controli l'accés del personal i autoritzi només els accessos que són estrictament necessaris per complir les tasques que té encomanades.

Q11. S'ha externalitzat alguna part del tractament a un encarregat?

Sí No

L'encarregat és la persona física o jurídica, autoritat pública, servei o organisme que presta al responsable un servei que comporta el tractament de dades personals per compte d'aquest. Per exemple, una empresa o entitat pública que ofereix un servei d'allotjament d'informació en els seus servidors o el gestor d'un servei públic municipal, entre d'altres supòsits.

L'externalització del tractament o part del tractament a un encarregat suposa una pèrdua de control sobre les dades. Cal escollir un encarregat que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures de seguretat apropiades, i definir clarament les seves responsabilitats.

Q12. Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD?

Sí No

Una manca de coneixements sobre l'ús que s'espera del sistema, sobre seguretat de la informació o sobre les obligacions i limitacions que imposa l'RGPD pot donar lloc a males pràctiques. Així, per exemple, el personal podria ser més propens a seguir les instruccions d'un correu de phishing o, a l'hora de desar documents, no ser conscient de garantir-ne la seguretat, entre d'altres situacions.

Altres característiques

Q13. Ha patit l'empresa o altres empreses del sector atacs darrerament?

Sí No

L'existència d'atacs anteriors ha de servir com a lliçó per identificar vulnerabilitats i reforçar la seguretat, així com d'advertència de potencials atacs futurs.

Altres característiques

<p>Q14. S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?</p> <p>La presència d'errors en el sistema de tractament incrementa la probabilitat de patir un atac. De la mateixa manera, les alertes o advertències respecte potencials fallades en la seguretat del sistema també poden indicar una probabilitat més alta de patir atacs.</p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>
<p>Q15. Es tracten dades d'especial interès o dades d'un nombre molt gran de persones usuàries?</p> <p>La presència massiva de dades i la presència de dades d'especial interès són una motivació extra per als possibles atacants.</p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>

Calculem la probabilitat inicial de en funció del nombre de respostes afirmatives d'acord amb la taula següent:

Respostes Afirmatives	Probabilitat Inicial
0 - 4	Baixa
5 - 9	Mitjana
10 - 15	Alta
Nombre de respostes afirmatives	
Probabilitat inicial estimada	

4.3 Risc inicial

Un cop estimat l'impacte i la probabilitat inicial, aplicarem la taula de la Secció 2.6 per calcular el risc inicial (sense els controls de seguretat).

Impacte sobre la confidencialitat	
Impacte sobre la integritat	
Impacte sobre la disponibilitat	
Màxim dels impactes	
Probabilitat	
Risc inicial	

4.4 Controls de seguretat

Un cop calculat el risc inicial, cal determinar quins controls (mesures per millorar la seguretat) s'han d'aplicar.

Hi ha moltes llistes de controls. Aquí fem ús dels controls de l'Esquema Nacional de Seguretat (RD 311/2024). Els controls de l'ENS són força complexos. A la Guia sobre l'AIPD trobareu indicacions i criteris per determinar quins aplicar.

Baix	Mitjà	Alt	Control	Aplicat
Marc organitzatiu				
Sí	Sí	Sí	Política de seguretat [org.1] (sistema)	
Sí	Sí	Sí	Normativa de seguretat [org.2] (sistema)	
Sí	Sí	Sí	Procediments de seguretat [org.3] (sistema)	
Sí	Sí	Sí	Procés d'autorització [org.4] (sistema)	
Marc Operacional				
Planificació				
Sí	Sí	Sí	Arquitectura de seguretat [op.pl.2] (sistema)	
Sí	Sí	Sí	Adquisició de noves components [op.pl.3] (sistema)	
Sí	Sí	Sí	Dimensionament [op.pl.4] (D)	
No	Sí	Sí	Components certificats [op.pl.5] (sistema)	
Control d'accés				

Baix	Mitjà	Alt	Control	Aplicat
Sí	Sí	Sí	Identificació [op.acc.1] (sistema)	
Sí	Sí	Sí	Requeriments d'accés [op.acc.2] (ICAT)	
No	Sí	Sí	Segregació de funcions i tasques [op.acc.3] (ICAT)	
Sí	Sí	Sí	Procés de gestió de drets d'accés [op.acc.4] (ICAT)	
Sí	Sí	Sí	Mecanisme d'autenticació per a usuaris externs [op.acc.5] (ICAT)	
Sí	Sí	Sí	Mecanisme d'autenticació per a usuaris interns [op.acc.6] (ICAT)	
Explotació				
Sí	Sí	Sí	Inventari d'actius [op.exp.1] (sistema)	
Sí	Sí	Sí	Configuració de seguretat [op.exp.2] (sistema)	
Sí	Sí	Sí	Gestió de la configuració de la seguretat [op.exp.3] (sistema)	
Sí	Sí	Sí	Manteniment i actualitzacions de seguretat [op.exp.4] (sistema)	
No	Sí	Sí	Gestió de canvis [op.exp.5] (sistema)	
Sí	Sí	Sí	Protecció contra codi maliciós [op.exp.6] (sistema)	
Sí	Sí	Sí	Gestió d'incidències [op.exp.7] (sistema)	
Sí	Sí	Sí	Registre de l'activitat de les persones usuàries [op.exp.8] (sistema)	
Sí	Sí	Sí	Registre de la gestió d'incidències [op.exp.9] (sistema)	
Sí	Sí	Sí	Protecció de Claus criptogràfiques [op.exp.10] (sistema)	
Serveis externs				
No	Sí	Sí	Contractació i acords de nivell de servei [op.ext.1] (sistema)	

Baix	Mitjà	Alt	Control	Aplicat
No	Sí	Sí	Gestió diària [op.ext.2] (sistema)	
No	No	Sí	Protecció de la cadena de subministrament [op.ext.3] (Sistema)	
No	Sí	Sí	Interconnexió de sistemes [op.ext.4] (sistema)	
Serveis en el núvol				
Si	Sí	Sí	Protecció dels Serveis en el núvol [op.nub.1] (sistema)	
Continuïtat del servei				
No	Sí	Sí	Anàlisi d'impacte [op.cont.1] (D)	
No	No	Sí	Pla de continuïtat [op.cont.2] (D)	
No	No	Sí	Proves periòdiques [op.cont.3] (D)	
No	No	Si	Mitjans alternatius [op.cont.4] (D)	
Monitorització del sistema				
Sí	Sí	Sí	Detecció d'intrusions [op.mon.1] (sistema)	
Sí	Sí	Sí	Sistema de mètriques [op.mon.2] (sistema)	
Sí	Sí	Sí	Vigilància [op.mon.3] (sistema)	
Mesures de protecció				
Protecció de les instal·lacions i les infraestructures				
Sí	Sí	Sí	Àrees separades i control d'accés [mp.if.1] (sistema)	
Sí	Sí	Sí	Identificació de les persones [mp.if.2] (sistema)	
Sí	Sí	Sí	Condicionament dels locals [mp.if.3] (sistema)	
Sí	Sí	Sí	Energia elèctrica [mp.if.4] (D)	
Sí	Sí	Sí	Protecció contra incendis [mp.if.5] (D)	

Baix	Mitjà	Alt	Control	Aplicat
No	Sí	Sí	Protecció contra inundacions [mp.if.6] (D)	
Sí	Sí	Sí	Registre d'entrada i de sortida d'equipament [mp.if.7] (sistema)	
Gestió del personal				
No	Sí	Sí	Caracterització del lloc de treball [mp.per.1] (sistema)	
Sí	Sí	Sí	Deures i obligacions [mp.per.2] (sistema)	
Sí	Sí	Sí	Conscienciació [mp.per.3] (sistema)	
Sí	Sí	Sí	Formació [mp.per.4] (sistema)	
Protecció dels equips				
Sí	Sí	Sí	Lloc de treball buidat [mp.eq.1] (sistema)	
No	Sí	Sí	Bloqueig del lloc de treball [mp.eq.2] (sistema)	
Sí	Sí	Sí	Protecció de portàtils [mp.eq.3] (sistema)	
Sí	Sí	Sí	Altres dispositius connectats a la xarxa [mp.eq.4] (C)	
Protecció de les comunicacions				
Sí	Sí	Sí	Perímetre segur [mp.com.1] (sistema)	
Sí	Sí	Sí	Protecció de la confidencialitat [mp.com.2] (C)	
Sí	Sí	Sí	Protecció de l'autenticitat i de la integritat [mp.com.3] (IA)	
No	Sí	Sí	Segregació de fluxos d'informació [mp.com.4] (sistema)	
Protecció dels suports de la informació				
Sí	Sí	Sí	Etiquetat [mp.si.1] (C)	
No	Sí	Sí	Criptografia [mp.si.2] (IC)	

Baix	Mitjà	Alt	Control	Aplicat
Sí	Sí	Sí	Custodia [mp.si.3] (sistema)	
Sí	Sí	Sí	Transport [mp.si.4] (sistema)	
Sí	Sí	Sí	Esborrat i destrucció [mp.si.5] (C)	
Protecció de les aplicacions informàtiques				
No	Sí	Sí	Desenvolupament d'aplicacions [mp.sw.1] (sistema)	
Sí	Sí	Sí	Acceptació i posada en servei [mp.sw.1] (sistema)	
Protecció de la informació				
No	Sí	Sí	Qualificació de la informació [mp.info.2] (C)	
Sí	Sí	Sí	Signatura electrònica [mp.info.3] (IA)	
No	No	Sí	Segells temporals [mp.info.4] (T)	
Sí	Sí	Sí	Neteja de documents [mp.info.5] (C)	
Sí	Sí	Sí	Còpies de seguretat [mp.info.6] (D)	
Protecció dels serveis				
Sí	Sí	Sí	Protecció del correu electrònic [mp.s.1] (sistema)	
Sí	Sí	Sí	Protecció de serveis i aplicacions web [mp.s.2] (sistema)	
Sí	Sí	Sí	Protecció navegació web [mp.s.3] (sistema)	
No	Sí	Sí	Protecció contra la denegació de servei [mp.s.4] (D) (impacte, probabilitat)	

4.5 Impacte residual

Els controls de seguretat poden reduir l'impacte d'un incident de seguretat. Per exemple, el xifratge de certa informació pot limitar l'extensió d'una pèrdua de confidencialitat, una còpia de seguretat pot limitar l'impacte d'una pèrdua de la disponibilitat de la informació i l'ús de signatura electrònica pot permetre la detecció, i per tant la reducció de l'impacte, d'una pèrdua de la integritat.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Impacte residual

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

--

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Impacte residual

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

--

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.

Impacte

--

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Impacte residual

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

--

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.

Impacte

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Impacte residual

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

Justificació

--

L'impacte residual del sistema serà el màxim dels tres anteriors.

Impacte residual del sistema

Baix	Mitjà	Alt	Molt Alt
------	-------	-----	----------

4.6 Probabilitat residual

Per reduir la probabilitat cal eliminar la casuística que fa que les preguntes de la secció 4.2 tinguin resposta afirmativa.

Moltes vegades no és factible eliminar la casuística associada a les preguntes de la secció 4.2. En aquest cas, per canviar una resposta afirmativa a negativa, cal justificar que, en el context del sistema de tractament, els controls implementats fan que l'objecte de la pregunta tingui un pes negligible en l'aparició d'incidents de seguretat.

Cal revisar les respostes donades en el càlcul de la probabilitat inicial tenint en compte els controls implementats.

Respondre només en aquelles preguntes on s'ha canviat la resposta, en base als controls que s'hagin implementat. S'han posat exemples de mesures de seguretat per justificar aquest canvi, sens perjudici que hi hagi altres controls que també puguin reduir la probabilitat.

Maquinari i programari

Q1	Està el sistema de tractament connectat a sistemes externs a l'organització?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q2	Alguna part del tractament es fa a través d'internet?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q3	Manca document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura de caràcter organitzatiu i de formació dels treballadors.	
Q4	Manca document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors i mesures relacionades amb la monitorització o registres.	
Q5	Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?	
	Controls implementats i justificació per reduir probabilitat	

Maquinari i programari

	Qualsevol mesura relacionada amb monitorització o registres.	
--	--	--

Procediments relacionats amb el tractament

	Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors?	
Q6	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura organitzativa i/o relacionada amb formació de treballadors.	
	Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?	
Q7	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors.	
	Pot el personal connectar dispositius externs al sistema?	
Q8	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
	Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?	
Q9	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	

Persones que intervenen en el tractament

	El personal rep permisos que no són necessaris per complir les tasques que té encomanades?	
Q10	Controls implementats i justificació per reduir probabilitat	

Persones que intervenen en el tractament

	Qualsevol mesura relacionada amb el control d'accessos i la formació als usuaris.	
	S'ha externalitzat alguna part del tractament a un encarregat?	
Q11	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
	Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD.	
Q12	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors.	

Altres característiques

	Ha patit l'empresa o altres empreses del sector atacs darrerament?	
Q13	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'han realitzat millores, en relació amb l'autenticació dels usuaris tant interns com externs, s'ha millorat la gestió d'incidents, s'ha millorat la vigilància i monitoratge dels sistemes o la pròpia xarxa corporativa.	
	S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?	
Q14	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'han millorat els procediments interns de seguretat, la gestió de configuració de la seguretat, o el sistema de mètriques.	
	Es tracten dades d'especial interès o dades d'un nombre molt gran de persones usuàries?	
Q15	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'ha millorat la gestió de configuració de la seguretat, o existència de sistemes redundants, o en general sistemes per a millorar la confidencialitat, la integritat o l'autenticitat.	

La probabilitat residual es calcula comptant el número de respostes afirmatives.

Respostes Afirmatives	Probabilitat inicial
0 - 4	Baixa
5 – 9	Mitjana
10 - 14	Alta

4.7 Estimació del risc residual

Un cop estimat l'impacte residual i la probabilitat residual, calculem el risc residual seguint la taula de la Secció 2.6.

Impacte				
Probabilitat	Baix	Mitjà	Alt	Molt Alt
Alta	Risc mitjà	Risc Alt	Risc Alt	Risc Alt
Mitjana	Risc baix	Risc mitjà	Risc Alt	Risc Alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc Alt

Impacte residual sobre la confidencialitat	
Impacte residual sobre la integritat	
Impacte residual sobre la disponibilitat	
Màxim dels impactes residual	
Probabilitat residual	
Risc residual	

Si el risc residual és alt, cal proposar nous controls per reduir-lo. Si no és possible reduir-lo, abans d'iniciar el tractament cal fer una consulta prèvia l'autoritat de protecció de dades competent sobre la seva idoneïtat.