UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Data: DD/MM/AAAA

Anàlisi de Riscos bàsica relativa a la Protecció de Dades Personals d'un treball acadèmic

Identificador del tractament	**F05.4** https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F05.4
Nom del tractament	Gestió de dades de projectes de Recerca i Innovació
Descripció de les finalitats del tractament	**Tractament de dades personals en treballs acadèmics.**

Nom del treball acadèmic

Índex

Aquesta anàlisi de riscos relativa a la protecció de dades personals (A**R**PD) és un procediment que cerca identificar i controlar el riscos pels drets i les llibertats de les persones que resulten d'un tractament de dades personals.

No cal fer una Avaluació d'Impacte de Protecció de Dades (A**I**PD) perquè no 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 A**I**PD.
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.

Ni dues o més de les següents característiques que poden ser indicatives de risc alt apliquen.

Indicador de potencial risc alt[1]
☐ Avaluació o puntuació, incloses l'elaboració de perfils i prediccions.
☐ Presa 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.
☐ Dades sensibles
☐ 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

CC BY NC

DOC 05022021

Document adaptat de les guies i plantilles proporcionades per l'Autoritat Catalana de Protecció de Dades
https://apdcat.gencat.cat/ca/documentacio/guies_basiques/Guies-apdcat/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

[1] Cal marca si aplica algun d'aquests indicadors. En el cas de que apliqui més d'un, caldrà fer una avaluació d'impacte, seguint aquesta guia https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf de l'Agencia Espanyola de Protecció de Dades, i formular consulta al Delegat de Protecció de Dades de la universitat (proteccio.dades@upc.edu)

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.

Nom del tractament

Finalitat del tractament

Descripció detallada de la finalitat del tractament

Responsable Intern / Interlocutors del tractament (Nom Cognoms + Unitat o Servei)

Ús de les dades personals amb propòsit diferent a de recol·lecció?	

☐ AUTOMATITZAT	☐ NO AUTOMATITZAT

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.

Categories de dades personals

☐ Caràcter identificatiu: Nom i cognoms; DNI/NIF/NIE/passaport; núm. SS; targeta sanitària; adreça postal, correu electrònic; telèfon (fix o mòbil); imatge; veu; marca física; signatura; empremta digital; signatura electrònica.

☐ Característiques personals: Dades d'estat civil; edat; dades de família; sexe; data de naixement; nacionalitat; lloc de naixement; llengua materna.

☐ Circumstàncies socials: Característiques d'allotjament, habitatge; propietats, possessions; aficions i estil de vida; esportives; pertinença a clubs, associacions; llicències, permisos, autoritzacions, identificador de xarxes socials.

☐ Acadèmiques i professionals: Formació; titulacions; historial d'estudiant; experiència professional; avaluació i mèrits; pertinença a col·legis o associacions professionals; idiomes o llengües.

☐ Detalls de l'ocupació: Cos/escala; categoria/grau; llocs de treball; dades no econòmiques de nòmina; historial del treballador.

☐ Dades d'informació comercial: Activitats i negocis; creacions artístiques, literàries, científiques o tècniques; llicències comercials; subscripcions a publicacions/mitjans de comunicació.

☐ Dades econòmico-financeres: Ingressos, rendes; inversions, béns patrimonials; crèdits, préstecs, avals; dades bancàries; plans de pensions, jubilació; dades econòmiques de nòmina; dades deduccions impositives/imposades; assegurances; hipoteques; subsidis, beneficis; historial crèdits; targetes crèdit; assegurances.

☐ Dades de transaccions: Béns i serveis subministrats per l'afectat; béns i serveis rebuts per l'afectat; transaccions financeres; compensacions/indemnitzacions.

☐ Dades de registre d'accés: Credencials d'usuari; IP i/o MAC; data i hora d'accés; webs accedides.

☐ Dades de naturalesa jurídica-administratives: Infraccions; sancions; dades penals; Administratives; víctima d'agressions; víctima de violència de gènere.

☐ Dades de categoria especial: Grau de discapacitat; salut; ideologia o opinions polítiques; afiliació sindical; origen racial o ètnic; biomètriques.

* Les dades especialment sensibles (en vermell) requeriran consulta al Delegat de Protecció de Dades.

Altres dades o categoria de dades personals:

Categoria de Dades	Dada personal

Procedència de les dades

☐ La persona interessada o el seu representant legal.
☐ Altres administracions públiques i entitats privades.
☐ Altres universitats públiques o privades.
☐ Altres:_____.

Procediment de recollida

☐ Formulari Paper.
☐ Formulari electrònic.
☐ Correu electrònic.
☐ Telèfon.
☐ Presencial.
☐ Dispositiu electrònic.
☐ Altres:_____.

Categories d'interessats

☐ Estudiants de la UPC
☐ Estudiants de secundària
☐ Estudiants d'altres universitats
☐ Futurs estudiants
☐ Antics estudiants
☐ Titulats i titulades
☐ Personal d'administració i serveis
☐ Personal docent i investigador
☐ Becaris d'aprenentatge, de doctorat o recerca
☐ Investigadors vinculats
☐ Persones que es connecten a la xarxa de telecomunicacions de la UPC
☐ Participants en seminaris, congressos, cursos i jornades
☐ Col·laboradors en seminaris, congressos i jornades
☐ Investigadors d'altres universitats, centres i altres entitats de recerca, nacionals o internacionals
☐ Representants d'empreses que participen en projectes de recerca
☐ Persones físiques identificables que accedeixen a espais o serveis de la UPC
☐ _____.
☐ _____.
☐ _____.
☐ _____.
☐ _____.
☐ _____.

Terminis de conservació de les dades

Les dades personals que es recullen i tracten s'han de conservar mentre sigui necessari per a els següents propòsits:

☐ Legal o normatiu:	Una llei o regulació fixa un període de retenció específic per a un tipus de registre particular.
☐ Evidència jurídica:	Els registres s'han de mantenir com a suport i evidència de contractes o altres drets i obligacions aplicables legalment, incloent-hi els períodes de prescripció per a l'acció judicial, el judici i l'execució de la sentència.
☐ Rendició de comptes financers:	S'han de mantenir els registres que documenten l'activitat financera que es requereixen per complir els requisits d'auditoria i impostos, i/o per mantenir una imatge financera precisa al llarg del temps.
☐ Reglament intern:	S'han de mantenir els registres per poder dur a terme l'auditoria interna i/o implementar la política d'arxiu.
☐ Necessitats contractuals:	S'han de mantenir els registres per donar suport a la gestió administrativa actual o futura, fins i tot com a element amb valor informatiu o de recerca a més llarg termini.
☐ Patrimoni:	Es poden mantenir els registres per raó de consideracions culturals i/o històriques perdurables.

Termini concret de conservació	_____ (dies o mesos o anys)

1.2 Actors no UPC que intervenen en el tractament. Encarregats de Tractament

Els actors no UPC que intervenen en el tractament, la seva funció i les dades que tracten són importants a l'hora de determinar els riscos del tractament.

Empresa o Entitat	
Processos en que intervé	
Encarregat o coResponsable	
País	

Empresa o Entitat	
Processos en que intervé	
Encarregat o coResponsable	
País	

1.3 Cessió o comunicació de dades

Destinatari	Descripció	Dades cedides o comunicades

Exemple:

Entitats bancàries ; Gestió el cobrament de la matrícula ; Dades identificatives, dades econòmico-financeres

1.4 Transferències Internacionals 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, el destinatari i la raó.

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?	Sí / 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 dels interessats pel tractament amb la nova finalitat.	Sí / No

Si no aplica la condició anterior, 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

Base legal pel tractament

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

L'interessat ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	Sí / No
El tractament és necessari per executar un contracte en què l'interessat n'és part o per aplicar mesures precontractuals.	Sí / No
El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.	Sí / No
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.	NO APLICA
El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.	Sí / No
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 l'interessat (en particular, quan l'interessat és un menor).	NO APLICA
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.

Tractament de dades de menors

Els **menors de 14 anys necessiten una protecció especial en el tractament de les seves dades**, perquè poden no ser conscients dels riscos que comporta.

Es tracten dades de menors de 14 anys?	Sí / No
En cas afirmatiu, s'haurà de demanar el consentiment als pares, mares o tutors legals	

Tractament de categories especials de dades

Es tracten dades de categories especials[1]?	Sí / No

En cas afirmatiu

El tractament de categories especials de dades està prohibit, llevat que apliqui algun dels supòsits següents.

L'interessat 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.	Sí / No
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.	Sí / No
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona, i l'interessat no està capacitat per donar el consentiment.	Sí / No
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.	Sí / No
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 dels interessats.	Sí / No
El tractament fa referència a dades que l'interessat ha fet públiques.	Sí / No
El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.	Sí / No
El tractament és necessari per raons d'interès públic essencial.	Sí / No
El tractament és necessari per a finalitats de medecina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social.	Sí / No
El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.	Sí / No
El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.	Sí / No
Justificació de la licitud del tractament de dades de categories especials.	

[1] El Reglament general de protecció de dades (RGPD) regula les categories especials de dades, que són les que revelen l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, dades relatives a la salut, a la vida sexual o a les orientacions sexuals d'una persona física. També el tractament de dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física.

Tractament de dades penals

Es tracten dades relatives a condemnes o infraccions penals , o sancions administratives?	Sí / 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.

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 els interessats de la possibilitat de retirar el consentiment en qualsevol moment.	

Transferències de dades

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

És fan transferències a tercers països o a organitzacions internacionals?	Sí / 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	
Condició que permet la transferència	

Dades transferides	
País	
Condició que permet la transferència	

Lleialtat del tractament

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

Es compleix aquest principi?	Sí / No

2.3 Principi de minimització

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

Es compleix aquest principi?	Sí / No

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.

Es compleix aquest principi?	Sí / No

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? etc.).

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.	Sí / No
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 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 l'eficàcia del tractament pel propòsit que és busca.

Justificació de la necessitat del tractament.

Justificació de que el tractament és proporcional

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 els interessats.

Tota comunicació amb els interessats ha de ser concisa, intel·ligible, de fàcil accés i ha de fer ús d'un llenguatge clar i senzill.	Sí / No

El reglament regula com s'ha de fer aquesta comunicació

La informació es donarà per escrit (incloent mitjans electrònics).	Sí / No
Pel cas de peticions fetes amb mitjans electrònics, la informació es donarà preferentment de forma electrònica.	Sí / No
Si l'interessat ho demana, la informació es donarà oralment.	Sí / No

El responsable ha de respondre les peticions d'exercici de drets d'un interessat dins uns terminis establerts:

Sense demora indeguda i no més enllà d'un mes.	Sí / 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.	Sí / No

Si el responsable no ha de respondre a la petició d'exercici de drets d'un interessat, cal:

Avisar l'interessat d'aquest fet sense demora indeguda i com a màxim en un mes.	Sí / No
Explicar les raons per no portar a terme la petició (per exemple, la petició és repetitiva o el responsable no pot identificar l'interessat).	Sí / No
Informar de la possibilitat de recorre la decisió davant una autoritat supervisora o un jutjat	Sí / No

Només si la petició és excessiva (per exemple, per repetitiva), es podrà cobrar un càrrec per cobrir els costos de tramitar-la.	Sí / No

3.2 Controls pel dret d'informació

A l'hora de recollir dades personals, el responsable del tractament ha d'informar els interessats de diferents aspectes del tractament.

Els articles 13 i 14, especifiquen que cal informar els interessats dels punts a la taula següent:

La identitat i les dades de contacte del responsable	Sí / No
Les dades de contacte del delegat de protecció de dades (si n'hi ha)	Sí / No
La finalitat del tractament	Sí / No
La base legal del tractament	Sí / No
L'interès legítim del responsable, si aquesta és la base legal del tractament	Sí / No
Els destinataris o categories de destinataris de les dades	Sí / No

El termini de conservació de les dades o el criteri emprat per determinar-lo	**Sí** / **No**
La intenció de transmetre les dades fora de la UE, si escau	**Sí** / **No**
La decisió de la Comissió Europea respecte de la suficiència de la seguretat que ofereix el país o organització destinatària	**Sí** / **No**
L'existència del dret d'accés a les dades	**Sí** / **No**
L'existència del dret de rectificació i supressió	**Sí** / **No**
L'existència del dret de limitació del tractament	**Sí** / **No**
L'existència del dret d'oposició al tractament	**Sí** / **No**
L'existència del dret de portabilitat de dades	**Sí** / **No**
L'existència del dret a revocar el consentiment (si aquesta és la base legal del tractament)	**Sí** / **No**
L'existència del dret a presentar una reclamació davant una autoritat de control	**Sí** / **No**
Que la comunicació de les dades és un requisit legal o contractual, si escau	**Sí** / **No**
L'existència de decisions automatitzades	**Sí** / **No**
El propòsit de fer servir dades amb una finalitat diferent a la que va motivar la recollida, si s'escau.	**Sí** / **No**
La procedència de les dades, si no s'han obtingut directament de la persona interessada.	**Sí** / **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 l'interessat, no hi ha l'obligació d'informar-lo si ja disposa de la informació.
- Si les dades no s'han obtingut directament de l'interessat, no cal informar-lo si es dona alguna de les següents condicions[1]: l'interessat 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?	**Sí** / **No**
Si aplica alguna exempció al dret d'informació, cal dir quina, a quines dades i justificar el perquè.	

Si s'informa els interessats, el Reglament determina quan cal fer-ho[2].

Si les dades es recullen directament dels interessats, en el moment de recollir-les.	**Sí** / **No**
Si les dades es recullen indirectament, cal complir les condicions següents:	
• En un període raonable de temps i no superior a un mes.	**Sí** / **No**
• Si ens comuniquem amb els interessats, com a molt tard en el moment de la primera comunicació.	**Sí** / **No**
• Si es volen comunicar les dades a tercers, abans de comunicar-les.	**Sí** / **No**

[1] RGPD, article 14.5.
[2] GDPR art 13(1) i 14(3),

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.

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 dels seus usuaris. • 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
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. Exemples de casos de pèrdua de la integritat: • Un empleat 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
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
Justificació

L'impacte del sistema serà el màxim dels tres.

Impacte ☐Baix ☐Mitjà ☐Alt

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	
P1. 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. Per exemple, la informació pot ser capturada o modificada maliciosament mentre està en trànsit. Exemples: • El sistema de tractament d'un hospital està connectat amb els sistema públic de seguretat social i amb els sistemes de d'asseguradores privades. • Les estacions de treball que formen part del sistema de tractament tenen accés a internet.	☐Sí ☐No

P2. Alguna part del tractament es fa a través d'internet? La interacció amb els interessats 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 els treballadors accedeixin al sistema de tractament a través d'internet també incrementa l'exposició a atacs externs i, a banda, incrementa la possibilitat que els treballadors facin un mal ús de la informació (accidental o intencionat). Exemples: • Botiga en línia, banca en línia, etc. • S'utilitza el correu electrònic en el tractament. • Els administradors del sistema de tractament poden fer tasques de manteniment o supervisió a través d'internet. L'accés al sistema de tractament des d'un espai públic pot facilitar que persones alienes a l'organització puguin observar-les	☐Sí ☐No
P3. Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament? 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. Hi ha multitud de guies de bones pràctiques en seguretat amb diferent temàtica (xarxa, equips, etc.). Exemples: • Cal dissenyar la xarxa seguint un document de bones pràctiques que inclogui elements com ara tallafocs, segmentació de la xarxa i ús de VPN. • Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el sistema operatiu. Això implica mesures com ara l'ús d'antivirus i no permetre l'ús de paraules de pas insegures. • Cal dimensionar el sistema de tractament pensant en les necessitats computacionals, de comunicació i d'emmagatzematge que s'anticipen. També cal dotar-lo del personal suficient. • Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el programari. Per exemple, com configurar un servidor web per fer-lo més segur. • Cal usar una metodologia de desenvolupament que tingui en compte la seguretat de les dades durant tot el cicle de vida de l'aplicació.	☐Sí ☐No

P4. Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament? És essencial fer un manteniment i una monitorització adequada del sistema. El manteniment s'ha de fer tant dels dispositius com del programari. Monitoritzar el sistema no només permet analitzar un incident un cop s'ha produït, sinó que també ajuda a detectar comportaments sospitosos a fi d'evitar que l'incident tingui lloc, o per reduir-ne l'impacte. Exemples: • No aplicar les actualitzacions de seguretat del sistema operatiu pot donar lloc a nous vectors d'atac. • La manca de còpies de seguretat regulars pot donar lloc a la pèrdua d'informació en cas d'incident.	☐Sí ☐No
P5. Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament? 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). Exemples: • El CPD no està degudament protegit amb un sistema que impedeix l'accés a les persones no autoritzades. • Les limitacions d'espai han fet que part de l'arxiu en paper s'hagi distribuït en diferents àrees, que no en garanteixen la seguretat. • El CPD no està protegit contra accidents naturals i industrials (per exemple, fallades elèctriques, inundacions). • És fa ús d'un servei al núvol sense tenir garanties que les instal·lacions proveïdor estan prou protegides.	☐Sí ☐No

Ús del sistema de tractament	
P6. Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors? 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). Exemples: • Un treballador d'una oficina bancària només hauria de consultar les dades dels seus clients. • Els treballadors són responsables de destruir la informació (digital o no) de forma segura, quan deixa de ser necessària. • Els treballadors són responsables de mantenir la seguretat de les dades, quan les comuniquen a alguna altra persona o organització.	☐Sí ☐No

P7. Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament? 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. Exemples: • La instal·lació de programari de compartició de fitxers pot donar lloc a la compartició involuntària de fitxers. • La instal·lació de programari per part d'usuaris no administradors pot donar lloc a un manteniment deficient. • Visitar pàgines web malicioses pot set una font d'entrada de programari maliciós i de robatori de dades.	☐Sí ☐No
P8. Pot el personal connectar dispositius externs al sistema? La connexió de dispositius externs al sistema de tractament és una porta a l'entrada de programari maliciós, d'introducció de vulnerabilitats, etc. A banda, també facilita l'extracció d'informació. Exemples: • El personal connecta el seu telèfon o el seu llapis de memòria als ports USB de l'ordinador. • El personal pot emprar els seus dispositius per efectuar tasques relacionades amb el tractament (BYOD).	☐Sí ☐No
P9. Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament? La manca d'un registre de les activitats (*log file*) pot incrementar les males pràctiques del personal i, alhora, dificulta la investigació dels incidents un cop s'han produït. Exemples: • Es poden consultar els expedients de clients/pacients sense que en quedi un registre. • Tot i que es genera un registre d'activitats, no es monitoritza. • No hi ha constància de les persones que entren al CPD.	☐Sí ☐No

Persones que intervenen en el tractament	
P10. El personal rep permisos que no són necessaris per complir les tasques que té encomanades? Com més gran sigui la base de persones que tenen accés a unes dades, més gran és la probabilitat que es produeixi un abús. Per evitar això, és essencial que el sistema controli l'accés al sistema del personal i autoritzi només els accessos que són estrictament necessaris per complir les tasques que té encomanades. Exemples: • L'accés a l'historial clínic d'un pacient hauria d'estar limitat als professionals que el tracten.	☐Sí ☐No

P11. S'ha externalitat alguna part del tractament a un encarregat? L'externalització del tractament o part del tractament a un encarregat suposa una pèrdua de control sobre les dades. Cal escollir un encarregat que pugui oferir un nivell alt de seguretat i definir clarament les seves responsabilitats. Exemples: • S'utilitza un núvol per realitzar part del tractament. • Es contracten uns serveis especialitzats per analitzar unes dades.	☐Sí ☐No
P12. 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? 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. Exemples: • La manca de coneixements en seguretat pot fer que el personal que tracta les dades sigui més propens a seguir les instruccions d'un correu de *phishing*. • El personal ha de recordar la necessitat de desar els document físics sota les condicions de seguretat adequades.	☐Sí ☐No

Altres característiques	
P13. Ha patit l'empresa o altres empreses del sector atacs darrerament? L'existència d'atacs anteriors s'ha de prendre com una advertència de potencials atacs futurs. Convé prendre les mesures necessàries per evitar que atacs similars tinguin èxit.	☐Sí ☐No
P14. S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament? La presència d'errors en el sistema de tractament incrementa la probabilitat de patir un atac. De la mateixa manera, les advertències respecte de potencials fallades en la seguretat del sistema també poden indicar una probabilitat més alta de patir atacs. Exemples: • En entrar dades incorrectes en un formulari, l'aplicació de tractament mostra un error i finalitza de forma inesperada. • S'ha rebut la notificació d'un usuari que el sistema és vulnerable a algun atac específic.	☐Sí ☐No
P15. Es tracten dades d'especial interès o dades d'un nombre molt gran d'usuaris? La presència massiva de dades i la presència de dades d'especial interès són una motivació extra per als possibles atacants. Exemple: • Una gran empresa que emmagatzema dades personals i financeres dels seus clients (per exemple, número de targeta de crèdit).	☐Sí ☐No

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 **PI**:	

4.3 Risc inicial

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

Per cadascun dels efectes negatius identificats, cal estimar el nivell de risc associat. El risc depèn de dos factors: l'impacte que té (baix, mitjà, o 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 circumstancies 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:

Probabilitat				
	Alta	Risc Mitjà	Risc Alt	Risc Alt
	Mitjana	Risc Baix	Risc Mitjà	Risc Alt
	Baixa	Risc Baix	Risc Baix	Risc Mitjà
		Baix	Mitjà	Alt
		Impacte		

Llevat que el risc sigui baix, cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar al Delegat de Protecció de Dades de la UPC (proteccio.dades@upc.edu) sobre la idoneïtat del tractament.

	PI * Valoració de l'Impacte
Impacte sobre la confidencialitat	Risc Baix / Mitjà / Alt
Impacte sobre la integritat	Risc Baix / Mitjà / Alt
Impacte sobre la disponibilitat	Risc Baix / Mitjà / Alt
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.

Si el tractament de dades personals és **NO AUTOMATITZAT** (paper), caldrà aplicar les següents mesures de seguretat:

Control	Aplicat
Existeix un control del personal que pot accedir als documents.	Sí/No
Identificació accessos per a documents accessibles per múltiples usuaris.	Sí/No
L'arxiu dels documents s'ha de fer segons criteris que facilitin la seva consulta i localització per garantir l'exercici dels drets d'accés, rectificació, supressió, limitació o oposició.	Sí/No
Dispositius d'emmagatzematge dotats de mecanismes que obstaculitzin la seva obertura.	Sí/No
Armaris, arxivadors de documents en àrees amb accés protegit mitjançant portes amb clau.	Sí/No
Durant la revisió o tramitació dels documents, la persona a càrrec dels mateixos ha de ser diligent i custodiar per evitar accessos no autoritzats.	Sí/No
La còpia o destrucció només pot realitzar-se pels usuaris autoritzats.	Sí/No
Destrucció de còpies rebutjades.	Sí/No
Mesures que impedeixin l'accés o manipulació en el trasllat de documentació.	Sí/No

Si el tractament de dades personals és **AUTOMATITZAT**, caldrà aplicar els controls definits en l'ENS (Esquema Nacional de Seguretat). Les respostes a aquests controls caldrà determinar-les amb els serveis TIC encarregats de desenvolupar o gestionar la plataforma i el sistema d'informació.

Baix	Mitjà	Control	Aplicat
Marc organitzatiu https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1074			
Sí	Sí	Política de seguretat [org.1] (sistema)	✓
Sí	Sí	Normativa de seguretat [org.2] (sistema)	✓
Sí	Sí	Procediments de seguretat [org.3] (sistema)	✓
Sí	Sí	Procés d'autorització [org.4] (sistema)	
Marc Operacional https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1079			
		Planificació	
Sí	Sí	Arquitectura de seguretat [op.pl.2] (sistema)	
Sí	Sí	Adquisició de noves components [op.pl.3] (sistema)	
No	Sí	Dimensionament [op.pl.4] (D)	
		Control d'accés	
Sí	Sí	Identificació [op.acc.1] (sistema)	
Sí	Sí	Requeriments d'accés [op.acc.2] (ICAT)	
No	Sí	Segregació de funcions i tasques [op.acc.3] (ICAT)	
Sí	Sí	Procés de gestió de drets d'accés [op.acc.4] (ICAT)	
Sí	Sí	Mecanisme d'autenticació [op.acc.5] (ICAT)	
Sí	Sí	Accés local [op.acc.6] (ICAT)	
Sí	Sí	Accés remot [op.acc.7] (ICAT)	
		Explotació	
Sí	Sí	Inventari d'actius [op.exp.1] (sistema)	

Sí	Sí	Configuració de seguretat [op.exp.2] (sistema)	
No	Sí	Gestió de la configuració [op.exp.3] (sistema)	
Sí	Sí	Manteniment [op.exp.4] (sistema)	
No	Sí	Gestió de canvis [op.exp.5] (sistema)	
Sí	Sí	Protecció contra codi maliciós [op.exp.6] (sistema)	
No	Sí	Gestió d'incidències [op.exp.7] (sistema)	
No	Sí	Registre de l'activitat dels usuaris [op.exp.8] (sistema)	
No	Sí	Registre de la gestió d'incidències [op.exp.9] (sistema)	
		Serveis externs	
No	Sí	Contractació i acords de nivell de servei [op.ext.1] (sistema)	
No	Sí	Gestió diària [op.ext.2] (sistema)	
No	Sí	Mitjans alternatius [op.ext.3] (D)	
		Continuïtat del servei	
No	Sí	Continuïtat del servei [op.cont.1] (D)	
Mesures de protecció https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1117			
		Protecció de les instal·lacions i les infraestructures	
Sí	Sí	Àrees separades i control d'accés [mp.if.1] (sistema)	
Sí	Sí	Identificació de les persones [mp.if.2] (sistema)	
Sí	Sí	Condicionament dels locals [mp.if.3] (sistema)	
No	Sí	Energia elèctrica [mp.if.4] (D)	
Sí	Sí	Protecció contra incendis [mp.if.5] (D)	
No	Sí	Protecció contra inundacions [mp.if.6] (D)	
Sí	Sí	Registre d'entrada i de sortida d'equipament [mp.if.7] (sistema)	
		Gestió del personal	
No	Sí	Caracterització del lloc de treball [mp.per.1] (sistema)	
Sí	Sí	Deures i obligacions [mp.per.2] (sistema)	
Sí	Sí	Conscienciació [mp.per.3] (sistema)	
Sí	Sí	Formació [mp.per.4] (sistema)	
		Protecció dels equips	
No	Sí	Lloc de treball buidat [mp.eq.1] (sistema)	
No	Sí	Bloqueig del lloc de treball [mp.eq.2] (sistema)	
No	Sí	Protecció de portàtils [mp.eq.3] (sistema)	
No	Sí	Mitjans alternatius [mp.eq.4] (D)	
		Protecció de les comunicacions	
Sí	Sí	Perímetre segur [mp.com.1] (sistema)	
No	Sí	Protecció de la confidencialitat [mp.com.2] (C)	
Sí	Sí	Protecció de l'autenticitat i de la integritat [mp.com.3] (IA)	
		Protecció dels suports de la informació	
Sí	Sí	Etiquetat [mp.si.1] (C)	
No	Sí	Criptografia [mp.si.2] (IC)	
Sí	Sí	Custodia [mp.si.3] (sistema)	
Sí	Sí	Transport [mp.si.4] (sistema)	
No	Sí	Esborrat i destrucció [mp.si.5] (C)	
		Protecció de les aplicacions informàtiques	
No	Sí	Desenvolupament d'aplicacions [mp.sw.1] (sistema)	
Sí	Sí	Acceptació i posada en servei [mp.sw.1] (sistema)	
		Protecció de la informació	
Sí	Sí	Qualificació de la informació [mp.info.2] (C)	

Sí	Sí	Signatura electrònica [mp.info.4] (IA)	
Sí	Sí	Neteja de documents [mp.info.6] (C)	
No	Sí	Còpies de seguretat [mp.info.7] (D)	
			Protecció dels serveis
Sí	Sí	Protecció del correu electrònic [mp.s.1] (sistema)	
Sí	Sí	Protecció de serveis i aplicacions web [mp.s.2] (sistema)	
No	Sí	Protecció contra la denegació de servei [mp.s.3] (D) (impacte, probabilitat)	

Director/a o ponent del treball acadèmic	**Estudiant/a**
Nom i Cognoms: Unitat o Servei: Data: Signatura:	Nom i Cognoms: Unitat Acadèmica: Data: Signatura: