

**20PR05 INFORME
D'AUDITORIA INTERNA**

**PROTECCIÓ DE DADES DE CARÀCTER
PERSONAL**

ÍNDEX

1. ANTECEDENTS, ORIGEN I OBJECTE DE L'AUDITORIA	2
1.1 Antecedents.....	2
1.2 Origen.....	2
1.3 Equip auditor.....	2
1.4 Objecte.....	2
2. MARC LEGAL.....	3
3. LA PROTECCIÓ DE DADES A LA UAB.....	3
3.1 Organigrama.....	3
3.2 Funcions del Delegat de Protecció de Dades.....	3
3.3 Responsables del tractament.....	4
3.4 Processos.....	4
4. ABAST I METODOLOGIA.....	5
4.1 Abast.....	5
4.2 Metodologia.....	5
4.2.1 Enquesta.....	5
5. ACTUACIONS REALITZADES, RESULTATS OBTINGUTS I OPORTUNITATS DE MILLORA.....	7
5.1 Anàlisi del grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament.....	7
5.1.1 Actuacions realitzades	7
5.1.2 Resultats obtinguts	8
5.1.3 Punts forts i oportunitats de millora.....	10
5.2 Revisió dels responsables del tractament de l'àmbit de la recerca.....	11
5.2.1 Actuacions realitzades	11
5.2.2 Resultats obtinguts	12
5.2.3 Punts forts i oportunitats de millora.....	12
5.3 Anàlisi de dades de categories especials sense tractament associat.....	13
5.3.1 Actuacions realitzades.....	13
5.3.2 Resultats obtinguts de la revisió de la població.....	13
5.3.3 Punts forts i oportunitats de millora.....	15
5.4 Anàlisi de dades biomètriques sense un tractament associat.....	15
5.4.1 Actuacions realitzades	15
5.4.2 Resultats obtinguts	16
5.4.3 Oportunitats de millora.....	17
5.5 Anàlisi dels protocols establerts pel que fa a les dades sobre la identitat de gènere.....	17
5.5.1 Actuacions realitzades	17
5.5.2 Resultats obtinguts	17
5.5.3 Oportunitats de millora.....	18
6. ALTRES ASPECTES REVISATS.....	19
6.1 Registre de violacions de seguretat	19
6.2 Aportacions generals de l'enquesta.....	19
6.3 Gestió i control de la documentació	19
6.4 Oportunitats de millora	20
7. OPINIÓ D'AUDITORIA.....	21
8. RESUM RESULTATS AUDITORIA.....	21
9. ANNEX.....	24

1. ANTECEDENTS, ORIGEN I OBJECTE DE L'AUDITORIA

1.1 Antecedents

El Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i la lliure circulació d'aquestes dades (RGPD) va eliminar l'obligació formal recollida a la legislació anterior de realitzar auditories biennals de protecció de dades.

Un dels principis que regeixen el tractament de dades personals en el RGPD és el de responsabilitat proactiva, en virtut de la qual el responsable del tractament (en aquest cas, la UAB) no només ha de complir amb les obligacions legals que li pertoquen, sinó que també ha d'estar en condicions de poder-ho demostrar.

En la gestió del compliment, l'auditoria és un instrument essencial, que permet, d'una banda, disposar d'evidències del compliment de les obligacions legals i, de l'altra, identificar les oportunitats de millora.

L'última auditoria obligatòria en protecció de dades, duta a terme per la UAB l'any 2016, va posar en relleu l'estat de compliment en la matèria i la necessitat de realitzar actuacions específiques de millora.

1.2 Origen

Per tal de documentar adequadament la implementació de les mesures que es van posar de manifest en aquella auditoria, es va proposar realitzar una **auditoria en protecció de dades de caràcter personal** que forma part de la programació anual de planificació d'auditories i que va ser aprovada per la Comissió Econòmica de Consell Social en data 11 de desembre de 2020 (CE 115/2020).

La promotora d'aquesta auditoria és la Secretària General, i l'encàrrec de projecte d'auditoria va ser validat l'1 de febrer de 2021. El Delegat de Protecció de Dades, d'ara en endavant DPD, ha estat designat el responsable del seguiment de pla d'acció que es derivi de l'Auditoria.

1.3 Equip auditor

L'equip auditor està format per la Sandra Flórez, tècnica de la Unitat d'Auditoria, la Laura Almendros, Cap de la Unitat d'Auditoria i pel Xavier Rubiralta, responsable de l'àmbit tecnològic en la protecció de dades.

1.4 Objecte

L'auditoria en protecció de dades de caràcter personal realitzada és una auditoria parcial i presenta els següents objectius:

- Analitzar el grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament.
- Revisió dels responsables del tractament de l'àmbit de la recerca.
- Anàlisi de dades de categories especials sense tractament associat.
- Anàlisi de dades biomètriques sense un tractament associat.
- Anàlisi dels protocols establerts pel que fa a les dades sobre la identitat de gènere.

El nostre treball respon, amb aquest informe, a la petició formulada.

L'Equip auditor agraeix la col·laboració del Delegat de Protecció de Dades per tota la documentació facilitada i l'assessorament proporcionat durant el transcurs de l'auditoria. També agraeix la col·laboració de la Unitat de Formació i Desenvolupament Professional, de l'Oficina de Coordinació Institucional, de les Administracions de Centre, de l'Administració de Serveis i Projectes específics, de l'Administrador d'espais de la zona cívica i del Servei de Seguretat i Vigilància, pel suport i ajut que ens han donat durant el transcurs de l'auditoria. També agraeix i valora molt positivament la col·laboració de les més de 900 persones que han respost l'enquesta per la informació proporcionada. Aquesta alta participació, atorga molta representativitat als resultats obtinguts a l'enquesta, els quals han estat analitzats en el marc de l'auditoria.

El treball de camp d'auditoria es va iniciar el 9 de març del 2021 i es va finalitzar el 21 de maig del 2021.

2. MARC LEGAL

El marc legal i normatiu consultat per a la realització d'aquesta auditoria ha estat el següent:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (Reglament General de Protecció de Dades), d'ara en endavant RGPD.
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals, en endavant LOPDGDD.
- Normativa per al Tractament de Dades de Caràcter Personal a la Universitat Autònoma de Barcelona, aprovada pel Consell de Govern el 17 de març de 2021.

3. LA PROTECCIÓ DE DADES A LA UAB

3.1 Organigrama

En compliment del que estableix el Reglament Europeu de Protecció de Dades (RGPD), la UAB va designar l'Agustí Verde Parera Delegat de Protecció de Dades de la UAB, en data 25 de gener de 2018.

El Delegat de Protecció de Dades de la UAB compta amb el suport de Xavier Rubiralta com a col·laborador, a temps parcial, en l'àmbit tecnològic i en la formació sobre la protecció de dades.

3.2. Funcions del Delegat de Protecció de Dades

Les principals funcions del Delegat de Protecció de Dades són les següents:

- Informar i assessorar els responsables o els encarregats i al personal de la UAB que s'ocupin del tractament de dades personals, de les obligacions que els pertoquen en virtut del RGPD i la resta de disposicions vigents en matèria de protecció de dades de caràcter personal.
- Supervisar el compliment del que estableix el RGPD i la resta de disposicions vigents en matèria de protecció de dades de caràcter personal, i de les polítiques de la UAB en aquest àmbit, inclosa l'assignació de

responsabilitats, la conscienciació i la formació del personal de la UAB que participi en operacions de tractament, i si s'escau, les auditories corresponents.

- Oferir l'assessorament necessari per als anàlisis de riscos i les avaluacions d'impacte relatives a la protecció de dades, i supervisar-ne l'aplicació.
- Cooperar amb l'Autoritat Catalana de Protecció de Dades, i actuar com a punt de contacte amb l'Autoritat per a qüestions referides al tractament de dades a la UAB.

En compliment de la Disposició Addicional Dissetena de la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), a la Comissió d'Investigació del dia 12 de febrer de 2020 es va acordar la incorporació del Delegat de Protecció de Dades a la Comissió d'Ètica en l'Experimentació Animal i Humana (a partir d'ara CEEAH). Aquesta participació permet la detecció del tractament de dades de caràcter personal des de l'inici dels projectes de recerca i contribueix a desplegar les mesures necessàries per tal d'aconseguir complir amb la legalitat vigent: designació de responsables funcionals del tractament, realització d'anàlisi de riscos, formalització de la documentació requerida legalment.

3.3. Responsables del tractament

El responsable del tractament és la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina el contingut, les finalitats i els mitjans del tractament. I està obligat a aplicar els principis del tractament (art. 5 RGPD), a analitzar les bases legitimadores del tractament (art. 6 RGPD), a dissenyar i aplicar les mesures de seguretat i a informar als interessats (art. 13 RGPD).

La UAB, com a persona jurídica, és el responsable dels tractaments que es fan. Però per a cada tractament en concret es nomena un o varis **responsables funcionals del tractament** que és qui assumeix les responsabilitats abans esmentades. En el cas de gestió son caps d'àrea, directors de servei, caps d'oficina o responsables d'unitat. I a l'àmbit acadèmic i de recerca son els investigadors principals, directors de tesi i tutors.

S'anomena tractament a "qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció".

A data de l'auditoria consten, a la Universitat, 110 responsables funcionals del tractament els quals gestionen 132 tractaments de dades de caràcter personal:

- 85 tractaments són de dades de recerca
- 47 tractaments són de dades de gestió

3.4. Processos

Durant el transcurs de l'auditoria s'ha detectat que caldria millorar la sistematització i la difusió dels processos relatius a la protecció de dades a la UAB. Això facilitaria les gestions i tràmits de tots els àmbits que intervenen en cada un dels processos, i agilitaria el seguiment.

Un dels processos principals que s'ha identificat és el que fa referència a la declaració de la responsabilitat d'un tractament de protecció de dades de caràcter personal. *Veure el workflow relatiu al procés a l'Annex.*

4. ABAST I METODOLOGIA

4.1 Abast

L'abast de l'auditoria són els cinc objectius especificats en el punt 1.4 (Objecte de l'auditoria) aplicats a la totalitat de tractaments de dades de caràcter personal que s'estan realitzant a la UAB en el moment de l'auditoria, independentment del grau de formalització d'aquests i del coneixement que en tinguí el Delegat de Protecció de Dades.

4.2 Metodologia

Les actuacions realitzades per a cada un dels objectius analitzats s'ha detallat a l'apartat corresponent, però a grans trets la metodologia emprada ha estat la següent:

- Realització d'una enquesta adreçada a tot el personal de la Universitat (PAS, PDI i PIF) amb la finalitat de recollir més informació.
- Revisió i anàlisi de les dades per tal de determinar el grau de compliment respecte el marc legal i/o normatiu corresponent.
- Per alguns dels objectius plantejats, s'ha obtingut la població i s'ha seleccionat i revisat una mostra, si s'ha considerat adient.
- Realització de consultes a alguns àmbits implicats.
- Formulació d'oportunitats de millora que formaran part de l'informe i del pla d'acció, a partir de la selecció dels resultats obtinguts

4.2.1 Enquesta

Tal i com s'ha indicat a la metodologia emprada, s'ha realitzat una enquesta adreçada a tot el personal de la Universitat amb la finalitat de poder recollir informació, de primera mà, de les persones que tracten amb dades de caràcter personal.

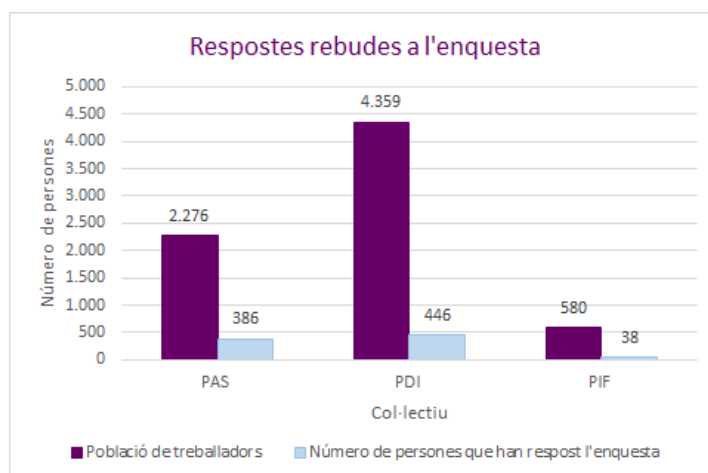
Per tal de recollir dades més específiques sobre les dades de categories especials, es va realitzar una enquesta específica destinada als 110 responsables funcionals del tractament.

Ambdues enquestes es van enviar el 9 de març del 2021, i van estar obertes durant 10 dies.

- L'enquesta general es va enviar a 7.100 persones (entre PDI, PAS i PIF) i es van rebre 870 respostes (12,25%).

Col·lectiu	Nombre de persones	Nombre de respostes de l'enquesta	% de respostes obtingudes
PAS	2.276	386	16,96%
PDI	4.359	446	10,23%
PIF	580	38	6,55%
TOTAL	7.100(*)	870	12,25%

(*) Del total de la població de treballadors hi ha 115 persones que són PAS i PDI a l'hora.



S'han classificat les respostes rebudes per àmbit de procedència:

Col·lectiu	Procedència	Respostes obtingudes
PAS	Serveis Centrals	118
	Departaments	89
	Gestions acadèmiques	36
	Biblioteques	35
	Instituts/Centres recerca	23
	Direcció TIC: APSI, Servei d'Informàtica, aules d'informàtica	23
	Servei de Llengües	16
	Administracions de centre	11
	Gestions econòmiques	8
	Slipi	7
	Serveis Científicotècnics	7
	Deganats	4
	SAF	3
	Servei d'ocupabilitat	3
	Altres serveis facultats	3
	Total PAS	386
PDI + PIF	Facultat de Filosofia i Lletres	81
	Facultat de Biociències	55
	Facultat de Ciències	52
	Escola d'Enginyeria	49
	Facultat de Ciències de l'Educació	36
	Facultat d'Economia i Empresa	34
	Facultat de Psicologia	31
	Facultat de Veterinària	31
	Facultat de Dret	27
	Facultat de Ciències de la Comunicació	23
	Facultat de Ciències Polítiques i de Sociologia	19
	Facultat de Medicina	17
	Facultat de Traducció i Interpretació	15
	Unitat docent Hospital del Mar	4
	Unitat docent Hospital de la Vall d'Hebron	4
	ICTA-ICP	4
	Unitat docent Hospital Sant Pau	1
	Unitat docent Hospital Germans Trias i Pujol	1
	Total PDI+PIF	484

- L'enquesta destinada als responsables funcionals del tractament es va enviar a 110 persones, que gestionen un total de 132 tractaments, i es van rebre 39 respostes (35,45%).

Tipologia del tractament	Nombre de tractaments	Nombre de responsables funcionals del tractament	Nombre de persones que han respost l'enquesta	% de respostes obtingudes
Recerca	85	66	18	27,27%
Gestió	47	45	21	46,67%
TOTAL	132	110 (*)	39	35,45%

(*) Hi ha un responsable que té tractaments de gestió i de recerca.

S'ha detectat que 12 responsables funcionals del tractament no van respondre l'enquesta específica com a responsables, però van respondre l'enquesta general. Les dades recollides de les seves respostes han estat tractades amb les de l'enquesta general.

5. ACTUACIONS REALITZADES, RESULTATS OBTINGUTS I OPORTUNITATS DE MILLORA

A continuació detallem les actuacions realitzades, els resultats obtinguts i les oportunitats de millora i punts forts detectats per cada un dels aspectes revisats que formen part de l'objecte de l'auditoria.

5.1. Anàlisi del grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament.

Tal i com es va definir a l'encàrrec de projecte, un dels objectius era el d'analitzar el grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament.

Una de les obligacions que imposa el RGPD és la formació i conscienciació del personal. En aquest sentit, a la UAB es duen a terme activitats formatives en matèria de protecció de dades des de principis de l'any 2000, amb l'entrada en vigor de la LOPD de 1999, i és a partir de 2013, quan es comencen a oferir unes sessions formatives més específiques associades al projecte del teletreball. Progressivament s'ha anat ampliant la oferta formativa amb la realització de cursos destinats a la formació específica per als responsables funcionals del tractament i d'altres destinats a la resta de treballadors de la universitat.

5.1.1 Actuacions realitzades

Per identificar quins responsables funcionals del tractament han rebut formació en matèria de protecció de dades, s'ha sol·licitat la informació de totes les activitats formatives en matèria de protecció de dades que s'han dut a terme a la UAB i/o que s'han vehiculat a través de la Unitat de Formació i Desenvolupament Professional entre el 16/05/2013 i el 27/11/2020.

S'han utilitzat les dades facilitades per l'Oficina de Coordinació Institucional per establir la població de treballadors de la UAB a data de març de 2021.

S'ha realitzat un anàlisi global de les dades amb l'objectiu de conèixer el grau de formació en matèria de protecció de dades del personal de la UAB i la tipologia de cursos que s'han realitzat.

També s'ha analitzat el grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament.

5.1.2 Resultats obtinguts

Anàlisi de la formació en protecció de dades

En primer terme, s'ha analitzat la població total que ha rebut formació en matèria de protecció de dades a través de la Unitat de Formació i Desenvolupament Professional. Des de l'any 2013 fins a l'abril de 2021 s'han format 1.039 persones.

Tenint en compte la població de PAS, PDI i PIF, el percentatge **del personal de la UAB format en matèria de protecció de dades és del 14,40%**. A continuació s'adjunta el detall per col·lectius:

Col·lectiu	Població de treballadors	Persones formades	% de persones formades
PAS	2.276	1.005	44,16%
PDI	4.359	33	0,76%
PIF	580	1	0,17%
TOTAL	7.215(*)	1.039	14,40%

(*)Del total de la població de treballadors hi ha 115 persones són PAS i PDI a l'hora.

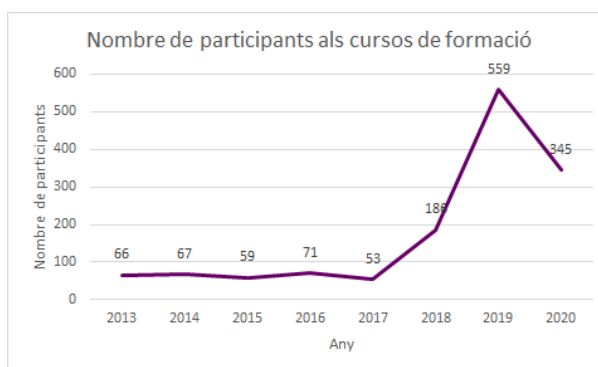
De les 1.039 persones que han realitzat formació en protecció de dades, s'han detectat 190 persones (18,29%) que no han realitzat formació posterior al 2018 i, per tant, a la UAB no li consta que hagin rebut formació del nou RGPD.

De les 1.005 persones del PAS que s'han format, un 42,59% (428 persones) la única formació en matèria de protecció de dades que han rebut, a través de la UAB, és la píndola formativa inclosa en el programa de teletreball i/o el curs de treball en remot (formació d'entre 1,25 i 1,5 hores).

El nombre de participants en els cursos de formació és de 1.406, mentre que les persones formades és de 1.039, ja que una persona pot haver realitzat més d'un curs de formació.

L'evolució del nombre de participants en les accions formatives en matèria protecció de dades ha estat la següent:

Any	Nombre de participants
2013	66
2014	67
2015	59
2016	71
2017	53
2018	186
2019	559
2020	345
TOTAL	1.406



Des de l'aparició del nou RGPD, al 2018, s'ha incrementat l'oferta formativa a la UAB. Durant els últims 3 anys s'ha format el 77,52% del total de participants.

La distribució dels participants per tipologia de programes formatius és la següent:

Modalitat	Curs de formació	Edicions	Hores de durada	Nombre de participants
INTERNA	ACOMPANYAMENT AL PROGRAMA DE TELETREBALL PER A PERSONES SUPERVISORES	4	1,5	14
	ACOMPANYAMENT AL PROGRAMA DE TELETREBALL PER A PERSONES TELETREBALLADORES	8	1,5	204
	LÍNIES BÀSIQUES DE LA PROTECCIÓ DE DADES PERSONALS. AUTOAPRENENTATGE VIRTUAL	3	10	19
	NORMATIVA EN PROTECCIÓ DE DADES DE CARÀCTER PERSONAL. ESPECIFICITATS EN UN ENTORN DE TREBALL EN REMOT (VIRTUAL)	3	1,5	156
	NORMATIVA EN PROTECCIÓ DE DADES DE CARÀCTER PERSONAL. ESPECIFICITATS PER TREBALLADORS EN RÈGIM DE TELETREBALL (VIRTUAL)	8	1,25	320
	NORMATIVA EN PROTECCIÓ DE DADES DE CARÀCTER PERSONAL. ESPECIFICITATS PER TREBALLADORS EN RÈGIM DE TELETREBALL.	3	1,25	65
	PROTECCIÓ DE DADES (RGPD) PER AL COL·LECTIU TÈCNIC DE LA DIRECCIÓ TIC	7	4	101
	REGLAMENT GENERAL DE PROTECCIÓ DE DADES (RGPD)	22	4	328
	REGLAMENT GENERAL DE PROTECCIÓ DE DADES (RGPD): VISIÓ GENERAL DELS IMPORTANTS CANVIS. EL RESPONSABLE DEL TRACTAMENT	5	2	66
	Total de participants a cursos interns			1273
EXTERNA	APLICACIÓ DEL REGLAMENT EUROPEU DE PROTECCIÓ DE DADES, PRIMERS PASSOS	1	4	4
	AUDITORIA DE SEGURETAT I PROTECCIÓ DE DADES	1	130	1
	CURS PROTECCIÓ DE DADES I RELACIONS LABORALS	1	50	1
	EL NOU REGLAMENT EUROPEU DE PROTECCIÓ DE DADES	1	9	1
	ELS REPTES DEL DRET A LA PROTECCIÓ DE DADES	1	2	1
	JORNADA: EINES PER AVALUAR L'ACOMPLIMENT DE LA NORMATIVA DE PROTECCIÓ DE DADES	1	2,5	3
	LA NOVA LLEI DE PROTECCIÓ DE DADES I LA FUNCIÓ DE PERSONES	1	2,5	5
	MOOC- TRANSPARÈNCIA I PROTECCIÓ DE DADES: INTERACCIÓ I EQUILIBRI	1	10	13
	PRINCIPALS NOVETATS DEL REGLAMENT EUROPEU DE PROTECCIÓ DE DADES	1	3,5	10
	PROTECCIÓ DE DADES PER A BIBLIOTECARIS	1	4	2
	REFORMA DE LA NORMATIVA EUROPEA DE PROTECCIÓ DE DADES	1	3	1
	REGLAMENT EUROPEU DE PROTECCIÓ DE DADES: PRINCIPIIS, DRETS I DEURES	1	3	1
	TRANSPARENCIA I PROTECCIÓ DE DADES: INTERACCIÓ I EQUILIBRI	1	10	19
	TRANSPARÈNCIA I PROTECCIÓ DE DADES: INTERACCIÓ I EQUILIBRI	1	10	68
	XV CICLE SEMINARIS UNIVERSITARIS. LA INCIDÈNCIA DEL REGLAMENT EUROPEU DE PROTECCIÓ DE DADES A LES EMPRESES	1	2	3
Total de participants a cursos externs				133

Dels 1.406 participants en els cursos de formació:

- 759 participants (un 53,98%) han fet algun dels cursos de formació destinats a les persones que participen al programa de teletreball o bé destinats al treball en remot (formació bàsica d'entre 1,25 hores i 1,5 hores) (ombrejats a la taula).
- 647 (un 46,02%) han fet altres cursos de formació la durada de les quals oscil·la entre 2 hores i 130 hores.

A través de l'enquesta realitzada s'han recollit 108 suggeriments que aporten valor sobre la formació i que poden ajudar a programar una oferta més ajustada a les necessitats dels usuaris pel que fa al contingut, el format, etc. La classificació dels comentaris ha estat la següent:

Tipus de comentari	Nombre
Formació més específica sobre alguns àmbits com per exemple el sanitari o bé formació amb experts.	14
Canvi del format de la formació, que sigui més pràctica, dinàmica, sempre disponible, online, etc.	13
Necessitat d'actualització del web sobre la protecció de dades o inclusió d'alguns continguts més dinàmics i accessibles: infografies, guia ràpida sobre tractament de dades, etc.	11
Increment de l'oferta formativa genèrica.	10
Necessitat d'oferta de formació de refresc o reciclatge.	10
Formació específica per al PDI sobre la publicació de notes d'alumnes i/o la gravació de classes.	10
Increment de l'oferta formativa adreçada al PDI, als PIF i als responsables de projectes.	9
Altres suggeriments sobre la formació.	9
Formació en protecció de dades obligatòria.	5
Formació pròpia rebuda per entitats externes.	5
Felicitació per la formació rebuda.	5
No es coneix l'oferta formativa.	4
A través de la formació rebuda no han obtingut resposta als seus dubtes i/o consultes plantejades	3
Total	108

Anàlisi de la formació rebuda pels responsables funcionals del tractament

D'altra banda, per avaluar el grau de compliment del RGPD pel que fa a la formació dels responsables funcionals del tractament, s'ha analitzat quins responsables s'han format en matèria de protecció de dades amb el programa específic de responsables del tractament.

Les dades es mostren a la següent taula:

Formació responsables funcionals del tractament	Recerca	Gestió	Total
Responsables que han rebut algun tipus de formació en matèria de protecció de dades	8	31	39
Han rebut formació específica per a responsables del tractament	8	20	28
Han rebut altres cursos de formació assimilables al de responsables del tractament	0	3	3
Han rebut únicament la píndola formativa dins del programa de teletreball i/o treball en remot	0	8	8
Responsables que no han rebut cap tipus de formació en matèria de protecció de dades	58	14	71
Nombre de responsables funcionals del tractament	66	45	110 (*)

(*) Hi ha un responsable que té tractaments de gestió i de recerca.

Dels 110 responsables funcionals del tractament:

- 31 responsables (un 28,18%) han rebut la formació específica i/o assimilable que exigeix el RGPD en matèria de protecció de dades.
- 79 responsables (71,82%) no han rebut la formació exigida pel RGPD en matèria de protecció de dades.

5.1.3 Punts forts i oportunitats de millora

Punts forts

- ✓ S'ha ampliat l'oferta formativa durant els últims anys, tant pel que fa als programes formatius específics adreçats als responsables funcionals del tractament, com pel que fa als programes formatius generals en matèria de protecció de dades.
- ✓ La centralització de la formació en una única unitat està contribuint a oferir un ventall més ampli de formació en matèria de protecció de dades destinats al col·lectiu PDI.

Oportunitats de millora

- **OM01:** Caldria fomentar i conscienciar de la importància de la protecció de les dades a tot el personal, a través de la formació, ja que són els dipositaris de les dades de caràcter personal que s'utilitzen a la Universitat:
 - Caldria potenciar i segmentar la formació oferta i garantir que aquesta estigui sempre disponible.
 - Caldria incorporar a la formació actual més accions formatives específiques que estiguin enfocades a les necessitats i temàtiques concretes dels col·lectius destinataris.
 - Caldria que la formació en protecció de dades fos obligatòria.
 - Caldria realitzar programes per garantir el reciclatge d'aquesta formació.
 - Caldria plantejar-se l'ampliació de contingut de la formació que es rep dins el programa de teletreball per fomentar la conscienciació de la protecció de dades, ja que des d'aquest programa es pot accedir a més personal.
 - Caldria formació específica sobre l'anonimització i la pseudo-anonimització de les dades. Aquestes mesures de protecció sovint són molt adequades en projectes de recerca, tant nacionals com europeus.
 - Caldria fer accions de divulgació i conscienciació per al professorat que planteja activitats als estudiants amb dades personals de categories especials, incidint en les seves obligacions com a responsables funcionals del tractament i de la necessitat de les garanties adequades.
- **OM02:** Caldria assegurar que un responsable funcional del tractament hagi realitzat la formació específica destinada als responsables abans de ser designat, ja que tot i que rep l'assessorament del DPD, cal complir amb les obligacions que imposa el RGPD sobre la formació i conscienciació del personal.

5.2 Revisió dels responsables del tractament de l'àmbit de la recerca.

A mitjans de la dècada dels noranta es va començar a desenvolupar la funció de protecció de dades a la UAB, en aplicació de les legislacions vigents en aquells moments (LORTAD i LOPD 1999). En un primer moment, els llavors anomenats fitxers, eren gairebé tots de l'àmbit de gestió i els de recerca es van anar incorporant paulatinament. La majoria de tractaments de dades de recerca, especialment els relacionats amb la investigació humana, impliquen el tractament de dades personals.

És per això que aquest punt es centra en analitzar els responsables del tractament de l'àmbit de recerca, per la seva importància i creixement, i per la tipologia de dades de caràcter personal tractades. A banda de la resta de les obligacions legalment establertes, és important identificar en cada cas la figura del responsable funcional del tractament, i assegurar que les dades de les persones afectades es tracten adequadament.

5.2.1 Actuacions realitzades

Les actuacions realitzades en aquest àmbit han estat les següents:

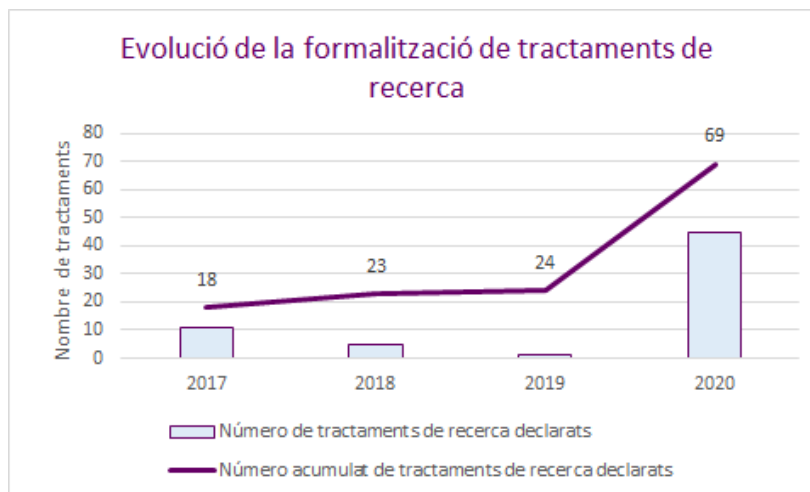
- S'ha observat la gestió dels responsables i tractaments, especialment els nomenaments, evolució en els col·lectius de gestió i recerca, i consideracions generals sobre la rellevància de l'àmbit de la recerca en la protecció de dades. La informació de partida han estat les respostes a l'enquesta adreçada als responsables funcionals del tractament i les dades dels tractaments de dades personals aportades pel DPD. En aquest apartat no s'ha abordat la formació dels responsables funcionals del tractament de l'àmbit de la recerca perquè ja s'ha tractat a l'apartat 5.1 de l'informe.

- S'ha analitzat l'estat i el grau de formalització de les designacions.
- S'ha fet un anàlisi del creixement dels tractaments de protecció de dades de l'àmbit de la recerca formalitzats en els darrers 5 anys.

5.2.2 Resultats obtinguts

- Del total de 132 tractaments, s'han detectat 95 que tenen formalitzada la designació del responsable funcional i 37 casos on aquesta encara no està formalitzada.
- S'ha detectat un creixement significatiu dels tractaments de protecció de dades de l'àmbit de la recerca, sobretot a partir de l'any 2020. La participació del Delegat de Protecció de Dades a la CEEAH podria ser la causa d'aquest increment ja que permet detectar de forma primerenca els projectes de recerca que impliquen tractament de dades personals. S'ha detectat un creixement en el primer quadrimestre del 2021 similar al de 2020.

Any	Número de tractaments de recerca declarats	Número acumulat de tractaments de recerca declarats	% increment
2017	11	18	61,11%
2018	5	23	27,78%
2019	1	24	4,35%
2020	45	69	187,50%



5.2.3 Punts forts i oportunitats de millora

Punts forts

- ✓ Des de la incorporació del DPD al CEEAH, aquest té constància de primera mà dels projectes de recerca en els quals es tractaran dades personals de categories especials, és a dir, és un punt detecció.

Oportunitats de millora

- **OM03:** Caldria habilitar algun mecanisme que permeti la detecció de tractaments de dades personals de categories especials, iniciats prèviament a la incorporació del Delegat de Protecció de Dades a la CEEAH, ja que en alguns casos el DPD no en té coneixement.
- **OM04:** Caldria regularitzar la situació dels tractaments que han passat a la CEEAH i que encara no tenen formalitzada la designació de responsable funcional.
- **OM05:** Caldria ampliar les accions específiques d'acompanyament i de suport als responsables funcionals del tractament de dades de l'àmbit de la recerca, ja que alguns d'aquests projectes presenten una sèrie de complexitats afegides: projectes comuns amb altres institucions, regulacions específiques en molts casos, treball de camp fora de la UAB i amb la intervenció de tercers, transferències internacionals de dades, persones que intervenen a la recerca amb diferents perfils i vinculació amb la UAB (per exemple, legislació biomèdica, enquestes pseudonimitzades, custòdia de mostres biològiques).

5.3 Anàlisi de dades de categories especials sense tractament associat.

Són dades de categories especials les d'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, les de salut, les d'afiliació sindical, les de vida o orientació sexual, les dades genètiques i les dades biomètriques amb finalitat d'identificació.

A l'auditoria del 2016 es van detectar, i durant aquests següents anys han anat apareixent, dades de categories especials sense tractament formalitzat. La finalitat, doncs d'auditar aquest àmbit rau en continuar amb la detecció de tractaments que continguin dades de categories especials de les que no s'ha identificat el seu tractament i per tant no s'ha comunicat al DPD, no s'ha formalitzat en el registre d'activitat de tractament (d'ara endavant RAT), no s'ha realitzat el corresponent anàlisi de riscos i no s'han aplicat les mesures de seguretat necessàries, amb els riscos que això comporta. L'absència de participació del DPD, pel fet de que no se li hagi informat, també implica que no es pugui analitzar si la finalitat del tractament justifica suficientment la utilització d'aquestes dades.

Cal tenir en compte que el tractament de dades de categories especials exigeix l'adopció de mesures de seguretat reforçades.

5.3.1 Actuacions realitzades

A través de les enquestes s'han recollit les dades de projectes tant en marxa com en fase d'estudi en els quals es tracten dades de categories especials.

De totes les respostes, s'han eliminat aquelles que no aporten valor o que no contenen dades de categories especials, i de la resta de respostes, s'ha consultat al DPD el grau de coneixement que té sobre aquests projectes.

Pel que fa als projectes futurs o en estudi que han de contenir aquest tipus de dades també s'ha cregut convenient analitzar la procedència de les respostes per àmbits així com classificar les respostes en funció de la tipologia de dades amb les que tracten.

5.3.2 Resultats obtinguts

L'enquesta ha fet aflorar l'existència d'alguns projectes, actuals o futurs, de tractaments que contenen dades de categories especials.

Projectes en marxa

S'han obtingut 122 respostes, de les quals 45 són de recerca (42,9%), 60 són de gestió (57,1%) i 17 respostes s'han exclòs perquè no corresponen a dades de categories especials.

S'ha analitzat el grau de coneixement que té el DPD sobre aquests projectes que contenen dades de categories especials:

Grau de coneixement que té el DPD	Recerca	Gestió	Total
Tractaments que estan formalitzats	28 (62,2%)	58 (96,7%)	86 (81,9%)
Tractaments que estan formalitzats però pendents d'alguna actualització de les dades	2 (4,4%)	1 (1,7%)	3 (2,9%)
Tractaments que no es poden identificar perquè no es disposa de suficient informació	11 (24,5%)	1 (1,7%)	12 (11,4%)
Tractaments no formalitzats	4 (8,9%)	0	4 (3,8%)
Total	45 (42,9%)	60 (57,1%)	105 (100%)

Nous projectes

S'han obtingut 56 respostes, de les quals 37 són de recerca (77,1%), 11 de gestió (22,9%) i 8 respostes que s'han exclòs perquè no aporten valor.

Les respostes del PDI provenen de dues grans àrees de coneixement: ciències socials (17) i ciències de la salut (20) tot i que en algun cas es barregen ambdues dimensions i és que l'àmbit de recerca és on hi ha gran part de les dades de categories especials. Està clar que en l'activitat investigadora de la UAB hi són ben presents les dades personals de categories especials, i que freqüentment són tractaments molt específics pel que fa a la protecció de dades personals i la seva regulació.

S'ha detectat que a les enquestes han aparegut alguns casos en els quals hi ha professors que plantegen activitats als estudiants on se'ls demanen o es tracten dades personals de categories especials i d'important sensibilitat.

S'ha analitzat el grau de coneixement que té el DPD sobre els nous projectes amb dades de categories especials comentats a l'enquesta:

Grau de coneixement que té el DPD	Recerca	Gestió	Total
Ha rebut informació al respecte i/o en té coneixement	8 (21,6%)	2 (18,2%)	10 (20,8%)
No ha rebut informació al respecte	28 (75,7%)	5 (45,5%)	33 (68,8%)
No hi ha prou informació a l'enquesta per poder-se pronunciar	1 (2,7%)	4 (36,4%)	5 (10,4%)
Total	37 (77,1%)	11 (22,9%)	48 (100%)

A continuació, es detallen les categories especials de l'àmbit de recerca, que han aflorat a l'enquesta, on es veu clarament la sensibilitat d'aquest tipus de dades i els riscos que pot comportar pel que fa als drets i llibertats dels interessats.

Àmbit	Tipologia de categories especials tractades en projectes de recerca	Nombre
Ciències Socials	Origen ètnic o racial/migració	6
	Gènere	3
	Actituds polítiques	3
	Violència en relacions interpersonals	2
	Creences religioses	1
	Orientació sexual	1
	Col·lectius vulnerables	1
Ciències de la Salut	Teràpies per malalties concretes	5
	Estudis clínics	4
	Psicopatologies	3
	Genètica	2
	VIH	2
	Persones intoxicades	1
	Persones amb discapacitat visual	1
	Salut en general	1
	COVID 19	1
Total		37

5.3.3 Punts forts i oportunitats de millora

Punts forts

- ✓ El fet que el PDI hagi aportat mitjançant l'enquesta gran part de la informació i amb detall sobre tractaments de dades de categories especials, evidencia la seva conscienciació, punt de partida per avançar en la protecció de dades a l'àmbit de recerca.

Oportunitats de millora

- **OM06:** Caldria habilitar a l'àmbit de la gestió, un punt de detecció de tractaments, anàleg a la participació del DPD a la CEEAH en l'àmbit de la recerca. No disposar de cap punt de detecció suposa un risc ja que no sempre es contemplarà adequadament la protecció de dades i per tant no es realitzaran els tràmits requerits legalment. (anàlisi de riscos, designació del responsable funcional del tractament, formalització del RAT, etc.)

5.4 Anàlisi de dades biomètriques sense un tractament associat

El RGPD defineix les dades biomètriques com dades personals obtingudes a partir d'un tractament específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permetin o confirmin la identificació única de la persona, com imatges facials o dades dactiloscòpiques.

Així mateix, quan les dades biomètriques s'utilitzen com a sistema d'identificació, el RGPD estableix a l'article 9 que es tracta de dades de categories especials.

5.4.1 Actuacions realitzades

Les actuacions realitzades s'agrupen en dos blocs:

- D'una banda s'han realitzat les comprovacions i les verificacions corresponents per tal de comprovar si les dades biomètriques que estan declarades compleixen amb tots els requisits exigits legalment:
 - S'han sol·licitat els registres d'activitat de tractament al Delegat de Protecció de Dades
 - S'ha comprovat la correcció de tota aquesta documentació.
- D'altra banda, s'han realitzat una sèrie d'accions adreçades a detectar àmbits de la UAB on es tracten dades biomètriques i s'ha comprovat si compleixen les formalitats legals necessàries. L'objectiu és el d'aflorar les dades on no s'està realitzant cap tractament associat per tal de poder desplegar accions que permetin regularitzar aquesta situació.
 - S'ha analitzat l'enquesta per detectar les respostes afirmatives a la pregunta si disposes en el teu àmbit de dades biomètriques i s'ha depurat la informació obtinguda analitzant les característiques o tipus de dades que indicaven tenir (s'han descartat aquelles respostes que un cop analitzat el tipus de dada es considerava que tècnicament no pertanyien a aquesta categoria).
 - S'ha enviat una petició a totes les Administracions de Centre per tal que informessin sobre quins dels seus àmbits i/o ubicacions disposen d'accessos que impliquin dades biomètriques.
 - S'ha consultat al Servei de Vigilància i Seguretat sobre aquells àmbits i/o ubicacions que disposen de sistemes d'accés amb dades biomètriques en base als seus registres, ja que aquest àmbit participa en el circuit d'alta d'instal·lació d'accessos.
 - En darrer lloc, s'ha recopilat tota aquesta informació i s'ha contrastat amb el Delegat de Protecció de Dades, per tal de comprovar si sobre aquestes dades s'ha realitzat algun tipus de tractament associat o formalització.

5.4.2 Resultats obtinguts

Durant l'auditoria, s'han detectat 26 sistemes de control d'accés que utilitzen dades biomètriques com a mètode d'identificació i pels quals no s'ha realitzat el registre d'activitat de tractament ni tampoc el tractament específic que, com a dades de categories especials, requeririen:

- 11 sistemes s'han detectat a través de les respostes obtingudes a l'enquesta.
- 15 sistemes s'han detectat a través de les consultes realitzades a les Administracions.

El nombre de sistemes de control d'accés que utilitzen dades biomètriques podria ser superior a 26 ja que poden haver-hi sistemes no detectats a través de les dues vies anteriors. Pel que fa a la consulta realitzada al Servei de Vigilància i Seguretat no hem obtingut resposta.

S'ha detectat que, en el circuit d'alta dels sistemes d'accés que requereixen de dades biomètriques per identificar-se, no es fa partícip al Delegat de Protecció de Dades i per tant aquest no té coneixement de l'existència d'aquestes dades. Aquest fet provoca que no es pugui activar el procés de designació de responsable funcional del tractament i per tant no es pugui formalitzar el registre d'activitat de tractament. La qual cosa acaba comportant un incompliment de les obligacions legals requerides per aquest tipus de dades.

Pel que fa a la revisió dels RAT's, en un dels casos la documentació és correcta i en l'altra cas no existeix RAT perquè es tracta d'un fitxer anterior al RGPD, inscrit al Registre de Protecció de Dades de l'Autoritat Catalana de Protecció de Dades, i el RAT està pendent de formalitzar-se.

5.4.3 Oportunitats de millora

- **OM07:** Caldria formalitzar els registres d'activitat de tractament corresponents a les dades biomètriques dels sistemes d'accés detectats durant l'auditoria. Aquests sistemes d'accés s'han instal·lat sense el coneixement ni l'assessorament del Delegat de Protecció de Dades.
- **OM08:** Caldria continuar amb la detecció de tractaments que contenen dades biomètriques, sobretot per la proliferació de sistemes d'accés que requereixen d'aquest tipus de dades per identificar-se, i que no tenen regularitzada la seva situació.
- **OM09:** Caldria incorporar, al procés de petició i instal·lació d'accessos d'identificació que utilitzen dades de tipus biomètric, la participació del Delegat de Protecció de Dades, perquè pugui designar, assessorar i formar els responsables funcionals corresponents, realitzar l'anàlisi de riscos i formalitzar la documentació que el RGPD exigeix.
- **OM10:** Seria recomanable actualitzar el registre corresponent al fitxer de dades biomètriques declarat a l'Autoritat Catalana de Protecció de Dades per convertir-lo en un RAT, perquè tot i que no és obligatori, permetria disposar de tota la informació dels tractaments en el mateix format (RAT's) així com, recollir les actualitzacions que el tractament pugui haver experimentat.

5.5 Anàlisi dels protocols establerts pel que fa a les dades sobre la identitat de gènere.

La identitat de gènere no pressuposa una específica orientació o preferència sexual, la qual cosa ha portat a la discussió doctrinal sobre la inclusió d'aquesta realitat entre les denominades dades de categories especials.

Aquesta qüestió pot afectar directament o indirectament als drets i les llibertats de les persones, per tant, és necessari que la UAB disposi de protocols específics i de mesures estrictes de seguretat i de confidencialitat, per tal de complir amb les exigències del RGPD en aquest àmbit.

És per això que s'ha considerat adient incloure aquest aspecte dins l'abast de l'auditoria.

5.5.1 Actuacions realitzades

Les actuacions realitzades en aquest àmbit es basen en l'anàlisi de les consultes realitzades als participants de l'enquesta sobre aquesta matèria:

- A l'enquesta adreçada a tota la població, s'ha informat als participants que la UAB disposa d'un protocol de canvi del nom legal al nom sentit i se'ls ha preguntat si coneixen els procediments establerts pel tractament d'aquestes dades, si han treballat mai amb aquest tipus de dades i si creuen que cal millorar algun aspecte relacionat amb el tractament d'aquestes dades.

5.5.2 Resultats obtinguts

Enquesta adreçada a tota el personal:

Pel que fa a la consulta sobre el **coneixement del procediment establert** pel tractament de dades referents al canvi de nom legal a nom sentit, el resultat és el següent:

Coneixement del procediment	Nombre de respostes	Rati
El coneix	150	17,24%
No el coneix	719	82,64%
No ha respost	1	N/A
TOTAL	870	14,40%

Pel que fa a la consulta sobre si **en el seu dia a dia treballen amb dades referents al canvi de nom legal a nom sentit**, el resultat és el següent:

Treballa en el seu dia a dia amb aquest tipus de dades	Nombre de respostes	Rati
Sí	99	11,38%
No	771	88,62%
TOTAL	870	14,40%

Per tal de determinar el risc que suposa que existeixi **personal que treballi habitualment amb aquest tipus de dades i no conegui el procediment establert**, s'ha creuat la informació obtinguda a les dues consultes anteriors i s'ha obtingut el resultat següent:

El personal que treballa habitualment amb aquestes dades, coneix el procediment?	Nombre de respostes	Rati
Sí	56	56,57%
No	43	43,43%
TOTAL	99	100%

Així doncs és rellevant destacar que el 56,57% del personal que treballa amb aquest tipus de dades coneix el protocol establert per la UAB mentre que el **43,43% no el coneix**.

Per tal de poder implementar millores en aquest camp s'ha consultat als enquestats si creien que caldria millorar algun aspecte pel tractament d'aquestes dades i s'ha obtingut un total de 63 aportacions que s'han agrupat per temàtiques.

Propostes de millora del procediment adreçades a:	Nombre d'aportacions
Augmentar la formació sobre el procediment, fer més difusió i que sigui més accessible	28
Expressar satisfacció sobre el funcionament del protocol tal i com està establert	4
Agilitzar el procediment perquè basant-se en els casos que han tramitat el consideren lent	4
Millorar la sincronització i actualització de les dades a les diferents aplicacions	5
Millorar la gestió i la seguretat de la informació associada amb el procediment	2
Possibilitar que el canvi de nom aparegui als llistats oficials d'alumnes	5
Altres	15

5.5.3 Oportunitats de millora

- **OM11:** Caldria donar a conèixer el Protocol de canvi del nom legal al nom sentit, i oferir una formació adient, ja que s'ha detectat que en molts àmbit es realitzen tràmits i gestions associades a aquest protocol i no es coneix prou bé el procediment establert.

6. Altres aspectes revisats

6.1 Registre de violacions de seguretat

L'article 35 del RGPD estableix que les violacions de seguretat s'han de notificar a l'Autoritat Catalana de Protecció de Dades en un termini màxim de 72 hores. Són exemples de violacions de seguretat la pèrdua, destrucció o alteració accidental o il·lícita de dades i suports, els accessos no autoritzats, impossibilitat d'accés de persones autoritzades, infeccions, compromís de contrasenyes i altres mecanismes d'autenticació, i incidents a la xarxa corporativa. Qui en sigui coneixedor ho ha de comunicar al responsable del tractament i aquest al Delegat de Protecció de Dades, qui en funció de la gravetat del incident decidirà si s'ha de comunicar al regulador. Per a cada tractament, el responsable d'aquest mantindrà un registre de les violacions de seguretat que han succeït on per cadascuna es guardarà la informació necessària.

S'ha analitzat el coneixement que té la població enquestada sobre el procediment de documentació i de comunicació i/o registre de violacions de seguretat i s'ha detectat que un 83,33% de les persones no coneixen aquest procediment.

Coneixen el procediment de comunicació i/o registre de violacions de seguretat	Nombre de persones	%
El coneix	145	16,67%
No el coneix	725	83,33%
Total	870	100,00%

6.2 Aportacions generals de l'enquesta

A través de la pregunta oberta de l'enquesta on els participants podien especificar tot allò que els interessava, els preocupava, etc., s'han recollit les següents aportacions classificades per temàtiques:

Aportacions generals	Nombre
Necessitat de conèixer els procediments existents, que aquests siguin més accessibles, responsabilitats.	24
Desconeixement del procediment de registre de violacions de seguretat o necessitat de tenir més informació sobre aquest.	23
Altres comentaris o observacions.	21
Necessitat de més formació.	11
Satisfacció o agraïment respecte les consultes efectuades o els procediments existents.	6
Realització de consultes relacionades amb la publicació de notes.	6
Necessitat d'aclarir aspectes específics sobre l'aplicació de la protecció de dades a algun àmbit concret: recerca, salut, drets d'imatge, etc.	4
Necessitat de simplificar procediments, fer-los més entenedors i/o disposar de més recursos en la protecció de dades.	3
Total	98

6.3 Gestió i control de la documentació

Durant el transcurs de l'auditoria s'han realitzat consultes i sol·licituds d'informació al Delegat de Protecció de Dades que han estat ateses de forma satisfactòria.

S'ha revisat la documentació rebuda i s'han detectat algunes oportunitats de millora pel que fa al format, a l'actualització i la custòdia dels registres dels tractaments.

6.4 Oportunitats de millora

Durant el transcurs de l'auditoria s'han detectat oportunitats de millora que no deriven directament dels objectius plantejats a l'auditoria però que es creu convenient indicar.

- **OM12:** Caldria fomentar la conscienciació i prioritització de la protecció de dades des de la direcció. La implicació en la protecció de dades ha de ser “universal”, és a dir, en tots els àmbits i a tots els nivells de lideratge. En un moment on la responsabilitat social, els ODSs i el Pacte Mundial de Nacions Unides són tan presents, els drets i llibertats de les persones de les que la UAB tracta les seves dades, han d'estar ben garantits.
- **OM13:** S'hauria de plantejar si la dotació de recursos actuals de suport a la protecció de dades és la necessària per donar compliment als requeriments legals, donat l'increment que s'està produint en el nombre de tractaments, l'especificitat d'algunes dades en l'àmbit de la recerca, l'exhaustivitat que requereix l'anàlisi de riscos i l'assistència individualitzada que s'està prestant als responsables funcionals del tractament.
- **OM14:** S'ha detectat que la col·laboració que està duent a terme el tècnic, que dona suport al DPD en l'àmbit tecnològic i en la formació en protecció de dades, no està formalitzada i per tant caldria analitzar la necessitat de regularitzar o formalitzar aquesta situació.
- **OM15:** Caldria formar, informar i conscienciar als responsables funcionals del tractament per tal que coneguin el procediment per documentar totes les violacions de seguretat que afectin les dades dels tractaments dels quals són responsables, tant si és preceptiu notificar-les a l'APDCAT com si no. En concret, s'ha de fer constar tota la informació relativa als fets, els efectes i les mesures correctores adoptades. Aquesta documentació ha d'estar a disposició de l'APDCAT (art. 33.5 RGPD).
- **OM16:** Caldria valorar la possibilitat d'introduir elements de transformació digital que permetin una automatització de certs tràmits pel que fa als procediments de designació dels responsables funcionals del tractament, anàlisi de riscos, etc.
- **OM17:** Seria necessari identificar i difondre els processos, i sistematitzar els tràmits relatius a la protecció de dades a la UAB. Això facilitaria les gestions i els tràmits de tots els àmbits que intervenen en cada un dels procediments, i agilitzaria el seguiment.
- **OM18:** Caldria introduir algunes millores en el control i gestió de la documentació associada als registres de tractaments de protecció de dades de caràcter personal que gestiona el DPD:
 - Caldria que tota la documentació relativa als tractaments de dades s'emmagatzemi en un repositori que garanteixi la seva integritat.
 - Caldria habilitar un sistema que permeti realitzar el seguiment de l'estat en que es troben els processos de tractament de dades de caràcter personal.
- **OM19:** Caldria millorar els canals d'informació en matèria de protecció de dades, actualitzar el repositori de materials disponibles i crear contingut més dinàmic a la web, amb l'objectiu de facilitar l'accés a la informació i resoldre els dubtes més freqüents.

7. OPINIÓ D'AUDITORIA

La nostra opinió pel que fa al compliment del RGPD per part de la UAB en el marc dels objectius plantejats a l'auditoria és favorable amb excepcions ja que s'han detectat una sèrie d'oportunitats de millora que s'haurien d'esmenar per evitar posar en risc aquest compliment.

En el transcurs de l'auditoria també s'han detectat i s'han posat de manifest oportunitats de millora fora de l'abast parcial de l'auditoria. També, s'han detectat altres aspectes que considerem que haurien de formar part de l'abast de futures auditories ja que esdevenen aspectes en els que caldria aprofundir:

- Anàlisi de riscos de tractaments i dels registres d'activitats de tractaments.
- Mesures de seguretat i protecció de dades de caràcter personal que afecten a l'àmbit de la Recerca i a les que l'Esquema Nacional de Seguretat no dona cobertura.
- Sistema de documentació, registre i notificació de les violacions de seguretat.
- El principi de minimització establert al RGPD ja que obliga a tractar només aquelles dades personals que siguin estrictament necessàries per a les finalitats del tractament, i la inclusió de dades innecessàries o excessives pot constituir un incompliment greu dels principis de protecció de dades.
- Traçabilitat de les dades d'una persona en tots els sistemes d'informació de la Universitat per poder donar una resposta completa als exercicis de dret dels interessats (accés, rectificació, supressió, oposició, limitació del tractament, portabilitat i dret a no ser objecte de decisions individuals automatitzades).

8. RESUM RESULTATS D'AUDITORIA

A continuació adjuntem un quadre resum amb les oportunitats de millora detectades durant l'auditoria i classificades segons la prioritització: Alta , Mitjana  o Baixa .

Oportunitat de millora	Prioritat
OM01: Caldria fomentar i conscienciar de la importància de la protecció de les dades a tot el personal, a través de la formació, ja que són els dipositaris de les dades de caràcter personal que s'utilitzen a la Universitat:	
Caldria potenciar i segmentar la formació oferta i garantir que aquesta estigui sempre disponible.	
Caldria incorporar a la formació actual més accions formatives específiques que estiguin enfocades a les necessitats i temàtiques concretes dels col·lectius destinataris.	
Caldria que la formació en protecció de dades fos obligatòria.	
Caldria realitzar programes per garantir el reciclatge d'aquesta formació.	
Caldria plantejar-se l'ampliació de contingut de la formació que es rep dins el programa de teletreball per fomentar la conscienciació de la protecció de dades, ja que des d'aquest programa es pot accedir a més personal.	
Caldria formació específica sobre l'anonimització i la pseudo-anonimització de les dades. Aquestes mesures de protecció sovint són molt adequades en projectes de recerca, tant nacionals com europeus.	
Caldria fer accions de divulgació i conscienciació per al professorat que planteja activitats als estudiants amb dades personals de categories especials, incidint en les seves obligacions com a responsables funcionals del tractament i de la necessitat de les garanties adequades.	
OM02: Caldria assegurar que un responsable funcional del tractament hagi realitzat la formació específica destinada als responsables abans de ser designat, ja que tot i que rep l'assessorament del DPD, cal complir amb les obligacions que imposa el RGPD sobre la formació i conscienciació del personal.	

OM03: Caldria habilitar algun mecanisme que permeti la detecció de tractaments de dades personals de categories especials, iniciats prèviament a la incorporació del Delegat de Protecció de Dades a la CEEAH, ja que en alguns casos el DPD no en té coneixement.	
OM04: Caldria regularitzar la situació dels tractaments que han passat a la CEEAH i que encara no tenen formalitzada la designació de responsable funcional.	
OM05: Caldria ampliar les accions específiques d'acompanyament i de suport als responsables funcionals del tractament de dades de l'àmbit de la recerca, ja que alguns d'aquests projectes presenten una sèrie de complexitats afegides: projectes comuns amb altres institucions, regulacions específiques en molts casos, treball de camp fora de la UAB i amb la intervenció de tercers, transferències internacionals de dades, persones que intervenen a la recerca amb diferents perfils i vinculació amb la UAB (per exemple, legislació biomèdica, enquestes pseudonimitzades, custòdia de mostres biològiques).	
OM06: Caldria habilitar a l'àmbit de la gestió, un punt de detecció de tractaments, anàleg a la participació del DPD a la CEEAH en l'àmbit de la recerca. No disposar de cap punt de detecció suposa un risc ja que no sempre es contemplarà adequadament la protecció de dades i per tant no es realitzaran els tràmits requerits legalment. (anàlisi de riscos, designació del responsable funcional del tractament, formalització del RAT, etc.)	
OM07: Caldria formalitzar els registres d'activitat de tractament corresponents a les dades biomètriques dels sistemes d'accés detectats durant l'auditoria. Aquests sistemes d'accés s'han instal·lat sense el coneixement ni l'assessorament del Delegat de Protecció de Dades.	
OM08: Caldria continuar amb la detecció de tractaments que contenen dades biomètriques, sobretot per la proliferació de sistemes d'accés que requereixen d'aquest tipus de dades per identificar-se, i que no tenen regularitzada la seva situació.	
OM09: Caldria incorporar, al procés de petició i instal·lació d'accessos d'identificació que utilitzen dades de tipus biomètric, la participació del Delegat de Protecció de Dades, perquè pugui designar, assessorar i formar els responsables funcionals corresponents, realitzar l'anàlisi de riscos i formalitzar la documentació que el RGPD exigeix.	
OM10: Seria recomanable actualitzar el registre corresponent al fitxer de dades biomètriques declarat a l'Autoritat Catalana de Protecció de Dades per convertir-lo en un RAT, perquè tot i que no és obligatori, permetria disposar de tota la informació dels tractaments en el mateix format (RAT's) així com, recollir les actualitzacions que el tractament pugui haver experimentat.	
OM11: Caldria donar a conèixer el Protocol de canvi del nom legal al nom sentit, i oferir una formació adient, ja que s'ha detectat que en molts àmbits es realitzen tràmits i gestions associades a aquest protocol i no es coneix prou bé el procediment establert.	
OM12: Caldria fomentar la conscienciació i prioritització de la protecció de dades des de la direcció. La implicació en la protecció de dades ha de ser "universal", és a dir, en tots els àmbits i a tots els nivells de lideratge. En un moment on la responsabilitat social, els ODS's i el Pacte Mundial de Nacions Unides són tan presents, els drets i llibertats de les persones de les que la UAB tracta les seves dades, han d'estar ben garantits.	
OM13: S'hauria de plantejar si la dotació de recursos actuals de suport a la protecció de dades és la necessària per donar compliment als requeriments legals, donat l'increment que s'està produint en el nombre de tractaments, l'especificitat d'algunes dades en l'àmbit de la recerca, l'exhaustivitat que requereix l'anàlisi de riscos i l'assistència individualitzada que s'està prestant als responsables funcionals del tractament.	
OM14: S'ha detectat que la col·laboració que està duent a terme el tècnic, que dona suport al DPD en l'àmbit tecnològic i en la formació en protecció de dades, no està formalitzada i per tant caldria analitzar la necessitat de regularitzar o formalitzar aquesta situació.	
OM15: Caldria formar, informar i conscienciar als responsables funcionals del tractament per tal que coneguin el procediment per documentar totes les violacions de seguretat que afectin les dades dels tractaments dels quals són responsables, tant si és preceptiu notificar-les a l'APDCAT com si no. En concret, s'ha de fer constar tota la informació relativa als fets, els efectes i les mesures correctores adoptades. Aquesta documentació ha d'estar a disposició de l'APDCAT (art. 33.5 RGPD).	
OM16: Caldria valorar la possibilitat d'introduir elements de transformació digital que permetin una automatització de certs tràmits pel que fa als procediments de designació dels responsables funcionals del tractament, anàlisi de riscos, etc.	
OM17: Seria necessari identificar i difondre els processos, i sistematitzar els tràmits relatius a la protecció de dades a la UAB. Això facilitaria les gestions i els tràmits de tots els àmbits que intervenen en cada un dels procediments, i agilitzaria el seguiment.	

OM18: Caldria introduir algunes millores en el control i gestió de la documentació associada als registres de tractaments de protecció de dades de caràcter personal que gestiona el DPD:	
Caldria que tota la documentació relativa als tractaments de dades s'emmagatzemin en un repositori que garanteixi la seva integritat.	
Caldria habilitar un sistema que permeti realitzar el seguiment de l'estat en que es troben els processos de tractament de dades de caràcter personal.	
OM19: Caldria millorar els canals d'informació en matèria de protecció de dades, actualitzar el repositori de materials disponibles i crear contingut més dinàmic a la web, amb l'objectiu de facilitar l'accés a la informació i resoldre els dubtes més freqüents.	

Bellaterra, juliol de 2021

Laura Almendros,
Cap de la Unitat d'Auditoria

9. ANNEX

Procés de declaració de la responsabilitat d'un tractament de protecció de dades de caràcter personal.

