Extracte del Reglament Intern sobre Protecció de Dades de Caràcter Personal aprovat pel Patronat de la Fundació UAB 13/05/2016

ÍNDEX

PREÀMBUL **Pàg. 3**

OBJECTE DEL REGLAMENT **Pàg. 3**

CREACIÓ, MODIFICACIÓ I SUPRESSIÓ DE FITXERS **Pag. 4**

- **CREACIÓ DE FITXERS** **Pàg. 4**
- **MODIFICACIÓ I SUPRESSIÓ DE FITXERS** **Pàg. 5**

RECOLLIDA, TRACTAMENT I CESSIÓ DE LES DADES **Pàg. 5**

- **RECOLLIDA DE LES DADES** **Pàg. 5**
- **TRACTAMENT DE LES DADES** **Pàg. 6**
- **CESSIÓ DE LES DADES** **Pàg. 6**
- **CONSERVACIÓ DE LES DADES** **Pàg. 7**

MESURES DE SEGURETAT **Pàg. 8**

DRETS DE LES PERSONES INTERESSADES: ACCÉS, CANCEL·LACIÓ, RECTIFICACIÓ I OPOSICIÓ **Pàg. 10**

- **DISPOSICIONS GENERALS** **Pàg. 10**
- **DRET D'ACCÉS** **Pàg. 11**
- **DRETS DE RECTIFICACIÓ, CANCEL·LACIÓ I OPOSICIÓ** **Pàg. 12**

DISPOSICIONS FINALS **Pàg. 13**

MESURES, NORMES, PROCEDIMENTS I REGLES DE SEGURETAT APLICABLES A FITXERS I TRACTAMENTS AUTOMATITZATS **Pàg. 14**

- **PLA DE SEGURETAT** **Pàg. 14**
- **IDENTIFICACIÓ I AUTENTICACIÓ** **Pàg. 14**
- **CONTROL D'ACCÉS I CONFIDENCIALITAT DE LA INFORMACIÓ** **Pàg. 14**
- **GESTIÓ DE SUPORTS** **Pàg. 15**
- **ÚS DE CORREU ELECTRÒNIC** **Pàg. 15**
- **ACCÉS A INTERNET** **Pàg. 16**
- **PROPIETAT INTEL·LECTUAL I INDUSTRIAL** **Pàg. 16**
- **FITXERS TEMPORALS** **Pàg. 17**

FUNCIONS I OBLIGACIONS DEL PERSONAL **Pàg. 18**

- **DE TOT EL PERSONAL** **Pàg. 18**
  - **Identificadors d'usuari i contrasenyes** **Pàg. 18**
  - **Utilització dels sistemes informàtics** **Pàg. 18**
  - **Confidencialitat de la informació** **Pàg. 19**
  - **Incidències** **Pàg. 20**
  - **Protecció de dades** **Pàg. 20**

PROCEDIMENT DE REGISTRE, NOTIFICACIÓ I RESPOSTA DE LES INCIDÈNCIES **Pàg. 22**

TIPOLOGIA DE LES INCIDÈNCIES **Pàg. 23**
REGISTRE D'INCIDÈNCIES **Pàg. 25**
MODEL PER AL REGISTRE D'INCIDÈNCIES **Pàg. 25**

ANNEXOS:

MODELS DE DOCUMENTS **Pàg. 26**

INFORMACIÓ A L'INTERESSAT **Pàg. 27**
PETICIÓ DRET D'ACCÉS **Pàg. 28**
PETICIÓ DRET DE RECTIFICACIÓ **Pàg. 29**
PETICIÓ DRET DE CANCEL·LACIÓ **Pàg. 30**
PETICIÓ DRET D'OPOSICIÓ **Pàg. 31**
NOTIFICACIÓ D'INCIDÈNCIA GENERAL **Pàg. 32**
NOTIFICACIÓ D'INCIDÈNCIA DE RECUPERACIÓ DE DADES **Pàg. 33**

PREÀMBUL

La Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant LOPD), i el Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, estableixen les obligacions que corresponen al responsable del fitxer de dades de caràcter personal, tant pel que fa a la creació dels fitxers, com a les persones responsables del tractament de les dades, les mesures de seguretat a adoptar, i els drets de les persones interessades, entre d'altres qüestions.

Amb la finalitat d'establir un marc de referència unívoc, clar i general per a la Fundació Universitat Autònoma de Barcelona (en endavant FUAB) i per a les institucions que dirigeix aquesta Fundació, es considera convenient articular un reglament intern que defineixi amb claredat els procediments, les competències i les responsabilitats en la matèria.

Així mateix, aquest reglament intern inclou, com a documents annexos un extracte del Document de Seguretat de la WASSU, així com els models necessaris per a la gestió de la protecció de dades.

CAPÍTOL I. OBJECTE DEL REGLAMENT INTERN

Article 1. Àmbit objectiu

1. Aquest reglament intern té com a objecte l'establiment de les obligacions principals que corresponen a la FUAB i/o a les institucions que dirigeix aquesta Fundació, en relació amb la creació dels seus fitxers de dades de caràcter personal, la recollida i el tractament de les dades, la seva eventual cessió, els procediments i les garanties per a l'exercici per part de les persones interessades dels drets d'accés, rectificació, cancel·lació i oposició, i la resta d'obligacions que li pertoquen d'acord amb la normativa de protecció de dades vigent.

2. Les disposicions d'aquest reglament intern fan referència a qualsevol fitxer amb dades de caràcter personal, sigui quina sigui la seva modalitat de creació, accés, organització i emmagatzematge.

Article 2. Conceptes

1. Constitueixen dades de caràcter personal qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables. S'entén que una persona és identificable quan la seva identitat pot determinar-se, directament o indirectament, a través d'un número d'identificació o mitjançant un o diversos elements específics característics de la seva identitat física, fisiològica, psíquica, econòmica, cultural o social.

2. Als efectes d'aquest reglament intern i del que preveu la legislació vigent en matèria de protecció de dades personals, el responsable del fitxer de dades personals és la FUAB i/o les institucions que dirigeix.

3. El responsable de seguretat és la persona a la que el responsable del fitxer ha assignat formalment la funció de coordinar i controlar les mesures de seguretat aplicables.

4. Als efectes del present reglament intern s'entendrà per responsable del tractament a aquella persona (o persones) a qui el responsable del fitxer ha delegat el control i la gestió del tractament del qual són responsables.

5. L'administrador del sistema és el responsable d'accedir al software del sistema, a les eines necessàries per al seu treball i als fitxers o bases de dades necessaris per resoldre els problemes que apareguin. Disposa dels màxims privilegis i, per tant, si una actuació errònia afecta el sistema, també és responsabilitat seva.

6. L'encarregat del tractament és la persona física o jurídica, l'autoritat pública, el servei o qualsevol altre organisme que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del fitxer.

7. S'entendrà per fitxer no automatitzat tot aquell conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat conforme a criteris específics relatius a persones físiques, que permetin accedir sense esforços desproporcionats a les seves dades personals, ja sigui centralitzat, descentralitzat o repartit de forma funcional o geogràfica.

CAPÍTOL II. CREACIÓ, MODIFICACIÓ i SUPRESSIÓ DE FITXERS

SECCIÓ PRIMERA. CREACIÓ DE FITXERS

Article 3. Autorització

La creació, la gestió, el desenvolupament i l'ús de qualsevol fitxer de dades de caràcter personal exigeix l'autorització prèvia de la Direcció Jurídica i de RRHH de la FUAB, en els termes i amb els límits que resulten de la legislació vigent en matèria de protecció de dades de caràcter personal i d'aquest reglament intern.

Article 4. Iniciatives de creació

1. Les institucions que vulguin crear i gestionar un fitxer de dades de caràcter personal hauran de trametre a la Direcció Jurídica i de RRHH de la FUAB una memòria on hi constaran, almenys, les informacions següents:

   - Nom del fitxer.
   - Descripció detallada de la finalitat i els usos previstos del fitxer.
   - Dades que composaran el fitxer.
   - Procediment de recollida de les dades.
   - Durada prevista del fitxer.
   - Suport, físic o lògic, del fitxer.
   - Cessions previstes de les dades.
   - Persona responsable del tractament.
   - Col·lectius dels que s'obtenen les dades
   - Procedència de les dades
   - Encarregat del tractament (si s'escau)
   - Cessions de dades (si s'escau)
   - Transferències internacionals (si s'escau)

Article 5. Procediment d'autorització

1. Les iniciatives i les sol·licituds per a la creació de fitxers de dades de caràcter personal seran trameses a la Direcció Jurídica i de RRHH de la FUAB, per a la

valoració de la seva conveniència i adequació a aquest reglament intern i a la legislació vigent en matèria de protecció de dades.

2. No podrà autoritzar-se, en cap cas, la creació de fitxers ni la recollida de dades personals que no tinguin una finalitat relacionada directament o indirectament amb les funcions i les competències pròpies de la FUAB i/o de les institucions que dirigeix aquesta Fundació.

SECCIÓ SEGONA. MODIFICACIÓ I SUPRESSIÓ DE FITXERS

Article 6. Modificació de fitxers

1. Qualsevol modificació en l'estructura, les finalitats o els usos dels fitxers autoritzats haurà de ser sol·licitada per la persona responsable del fitxer a la Direcció Jurídica i de RRHH de la FUAB, amb l'especificació de les parts que n'hagin de resultar modificades.

2. No s'autoritzarà cap modificació que contingui previsions contràries als principis de consentiment, qualitat, finalitat, actualitat i exactitud de les dades, o a qualsevol altre principi establert a legislació vigent en matèria de protecció de dades.

Article 7. Supressió de fitxers

1. La persona responsable del fitxer, quan consideri que algun fitxer ha deixat de ser útil a les finalitats per a les quals va ser creat o per a l'acompliment de les funcions pròpies de la institució, en sol·licitarà la supressió a la Direcció Jurídica i de RRHH de la FUAB, amb expressió de les causes que motiven la sol·licitud.

CAPÍTOL III. RECOLLIDA, TRACTAMENT I CESSIÓ DE LES DADES

SECCIÓ PRIMERA. RECOLLIDA DE LES DADES

Article 8. Qualitat de les dades

1. Les dades de caràcter personal recollides per la FUAB i/o les institucions que dirigeix aquesta Fundació en qualsevol dels seus fitxers degudament autoritzats, seran adequades, pertinents i no excessives en relació amb les finalitats per a les quals hagin estat creats els fitxers.

2. En el moment de la recollida de les dades, les persones interessades hauran de ser informades, almenys, dels aspectes següents:
   - L'existència d'un fitxer de dades, identificant-lo sempre que sigui possible, i les seves finalitats.
   - El caràcter obligatori o facultatiu de la resposta a les qüestions que li siguin plantejades, així com les conseqüències de la negativa a facilitar les dades.
   - La facultat d'exercir els drets d'accés, rectificació, cancel·lació i oposició, quan escaigui, així com el lloc i el mecanisme establert per a l'exercici d'aquests drets.
   - La identitat i adreça del responsable del fitxer.

3. Aquesta informació ha de ser facilitada a través d'algun mitjà que permeti acreditar que s'ha facilitat aquesta informació. La persona responsable del tractament ha de conservar el suport en què consti el compliment del deure d'informar. Per a l'emmagatzematge dels suports, la persona responsable del tractament pot utilitzar

mitjans informàtics o telemàtics. En particular pot escanejar la documentació en suport de paper, sempre que es garanteixi que en l'esmentada automatització no s'ha produït cap alteració dels suports originals.

4. Quan les dades no hagin estat obtingudes directament de les persones interessades, aquestes hauran de ser informades de manera expressa, inequívoca i precisa de les circumstàncies exposades en l'apartat 2 d'aquest article, llevat dels supòsits que, d'acord amb la legislació vigent, el consentiment no sigui preceptiu.

SECCIÓ SEGONA. TRACTAMENT DE LES DADES

Article 9. Ús de les dades

Les dades de caràcter personal seran destinades exclusivament a les finalitats per a les quals han estat recollides.

Article 10. Consentiment

1. El consentiment de les persones interessades serà necessari per al tractament de les seves dades personals, excepte en els supòsits previstos expressament a la legislació vigent en matèria de protecció de dades.

2. El consentiment podrà ser exprés o tàcit, llevat dels casos en què la legislació vigent en matèria de protecció de dades exigeixi formalitats específiques en el seu atorgament.

Article 11. Actualització de les dades

La persona responsable del tractament garantirà l'actualització permanent dels fitxers de dades de caràcter personal de la institució corresponent.

Article 12. Cancel·lació de dades

Les dades de caràcter personal seran cancel·lades quan hagin deixat de ser útils a les finalitats per a les quals varen ser recollides.

SECCIÓ TERCERA. CESSIÓ DE LES DADES

Article 13. Supòsits de cessió

Les dades de caràcter personal només podran ser cedides en els supòsits en què la cessió estigui expressament autoritzada per llei, i en aquells casos en què s'hagi previst expressament en el moment de la creació del fitxer de dades corresponent. Qualsevol altra cessió requerirà el consentiment previ de la persona interessada.

Article 14. Procediment de cessió

Qualsevol demanda de dades de caràcter personal a la FUAB i/o a les institucions que dirigeix aquesta Fundació per part d'altres entitats o d'organismes públics o privats, haurà de ser comunicada a la Direcció Jurídica i de RRHH de la FUAB.

Article 15. Accés de terceres persones a les dades

Les empreses, entitats i organismes de naturalesa pública i privada que tinguin contractat un servei amb la FUAB i/o amb les empreses que dirigeix aquesta Fundació, podran

accedir a les dades personals dels diversos fitxers quan això sigui necessari per al desenvolupament i execució del contracte subscrit.

Els contractes, que s'hauran de formalitzar per escrit, hauran d'especificar clarament el seu objecte, preveure les dades de caràcter personal necessàries a les que podrà tenir accés el contractista i les condicions en què podrà tractar-les, i especificar el compromís del contractista de complir i respectar les exigències de la legislació en matèria de protecció de dades, així com trametre a la institució corresponent la documentació acreditativa de l'adopció de les mesures de seguretat exigides per la legislació vigent. En el cas que es prevegi la possibilitat que l'encarregat del tractament pugui subcontractar la totalitat o part del servei encarregat s'haurà de fer constar aquesta possibilitat en el contracte de prestació de serveis.

De conformitat amb el que preveu la legislació vigent en matèria de protecció de dades de caràcter personal, la comunicació de dades personals a què fa referència aquest article no té la consideració de cessió, i no requereix, per tant, el consentiment de la persona interessada.

SECCIÓ QUARTA. CONSERVACIÓ DE LES DADES

Article 16. Conservació de les dades

Les dades de caràcter personal es conservaran mentre siguin necessàries per a la finalitat de la seva recollida.
Quan deixin de ser necessàries per a la finalitat que va motivar la seva recollida es conservaran, no accessibles, durant els terminis establerts legalment.

Article 17. Arxiu documental

Si es tracta de dades personals emmagatzemades en suports no automatitzats (suport paper), es procedirà al seu trasllat a l'arxiu departamental per al seu arxiu definitiu.
Només podran accedir a l'arxiu departamental aquells usuaris autoritzats pel director del departament corresponent.

Article 18. Préstec d'informació de l'arxiu

1. Quan un usuari autoritzat necessiti documents amb dades de caràcter personal que es trobin en l'arxiu definitiu, procedirà a retirar la documentació necessària, tot deixant en el lloc ocupat per aquesta documentació un document (mòmia) en el que s'indiqui la documentació retirada, la identificació de qui l'ha retirat i la data en que s'ha retirat aquesta documentació. Un cop acabat el tractament de la informació retirada, es procedirà a retornar-la a l'arxiu departamental, tot substituint el document mòmia deixat en l'arxiu per la documentació original.

2. Quan l'usuari que necessiti accedir temporalment a la informació emmagatzemada en l'arxiu departamental, no sigui un usuari autoritzat, haurà de sol·licitar l'autorització del director del departament corresponent.

Article 19. Accés de terceres persones a l'arxiu documental

Per a que una persona externa a la FUAB i/o a les institucions que dirigeix aquesta Fundació pugui tenir accés als arxius departamentals, haurà d'estar prèviament autoritzada pel director del departament corresponent.

El personal extern sol·licitarà accés a l'arxiu departamental segons el procediment establert en l'article 20 d'aquest reglament.

Article 20. Autorització d'accés

1. Quan una persona no autoritzada necessiti accedir a un arxiu documental haurà d'obtenir l'autorització del director del departament al que pertany l'arxiu documental al que es necessita accedir.

2. Per a poder obtenir la corresponent autorització es dirigirà al director del departament tot motivant la necessitat d'accés a l'arxiu, quedant a criteri del director l'atorgament de l'autorització sol·licitada. Si el director concedeix l'autorització d'accés a l'arxiu documental, expedirà un document en el que s'indiqui arxiu al que es concedeix l'accés, persona o persones a les que es concedeix l'accés, finalitat de l'accés i període de temps en el que és vàlida l'autorització atorgada.

3. El sol·licitant haurà de conservar el document d'autorització mentre aquesta estigui en vigor.

CAPÍTOL IV. MESURES DE SEGURETAT

Article 21. Nivells de seguretat

1. De conformitat amb el que disposa la legislació vigent, les mesures de seguretat dels fitxers de dades de caràcter personal es classifiquen en tres nivells: bàsic, mitjà i alt, en funció de la naturalesa de la informació tractada, i en relació amb la major o menor necessitat de garantir la confidencialitat i la integritat de la informació.

2. Tots els fitxers de dades de caràcter personal han d'adoptar, almenys, les mesures de seguretat de nivell bàsic.

3. Els fitxers que continguin dades relatives a la hisenda pública, serveis financers, solvència econòmica i aquells que mantinguin dades suficients per avaluar la personalitat de la persona interessada exigiran mesures de seguretat de nivell mitjà.

4. Els fitxers que continguin dades relatives a la ideologia, religió, creences, origen racial, vida sexual i salut exigiran mesures de seguretat de nivell alt.

5. L'establiment d'aquests nivells de seguretat és d'aplicació tant als fitxers automatitzats (informatitzats) com als fitxers no automatitzats (fitxers en paper).

6. El responsable del fitxer, el responsable de seguretat i l'administrador del sistema i, si s'escau, la persona responsable del tractament, tenen la responsabilitat de vetllar, en el seu àmbit respectiu, pel compliment de les mesures de seguretat que corresponguin al nivell de seguretat del fitxer.

Article 22. Document de seguretat

1. D'acord amb el que determina la legislació vigent en matèria de protecció de dades, la FUAB ha elaborat i aprovat un document de seguretat per als seus fitxers de dades de caràcter personal, així com els de les institucions que dirigeix aquesta Fundació.

2. El manteniment, les revisions i les actualitzacions del document de seguretat corresponen al responsable de seguretat d'ofici o a instància de les persones responsables del tractament.

Article 23. Personal al servei de la FUAB i/o al de les institucions que dirigeix aquesta Fundació

1. Les persones que prestin els seus serveis en la FUAB i/o en les empreses que dirigeix aquesta Fundació hauran de ser informades de les obligacions que els pertoquen pel que fa a les mesures de seguretat i el deure de secret, d'acord amb el que preveu el document de seguretat.

2. Els documents en què es formalitzi la incorporació de persones per prestar serveis a la FUAB i/o a les institucions que dirigeix aquesta Fundació, inclouran l'advertiment sobre les obligacions que corresponen a les persones que hagin de tenir accés a fitxers de dades de caràcter personal. Així mateix, les persones que s'incorporin a alguna d'aquestes institucions hauran de signar un document de compromís en aquest sentit.

Article 24. Fitxers no automatitzats amb dades de caràcter personal

1. Els fitxers no automatitzats han de complir, igual que els fitxers automatitzats, amb el que estableix la LOPD i el RLOPD. Per tant, a l'igual que per als fitxers automatitzats, el responsable del fitxer, haurà de garantir que es compleixen els extrems establerts en l'article 9 d'aquest reglament.

2. Tots els fitxers no automatitzats que contenen dades de caràcter personal hauran de complir amb un subconjunt de les mesures de seguretat establertes per als fitxers automatitzats. En concret les referents a funcions i obligacions del personal, registre d'incidències, control d'accés i gestió de suports.

3. Als fitxers no automatitzats de nivell bàsic se'ls hauran d'aplicar mesures de seguretat relacionades amb:

    a. Establir un procés per al trasllat de la documentació a l'arxiu departamental.
    b. Emmagatzematge de documents amb dades de caràcter personal: els documents que contenen dades de caràcter personal s'emmagatzemaran en armaris que disposin d'algun mecanisme que dificulti la seva obertura.
    c. Custòdia de documents no emmagatzemats: respecte de la documentació no emmagatzemada en armaris (documentació amb la que s'està treballant), serà responsabilitat de la persona que n'estigui al càrrec, garantir que només puguin tenir accés a la documentació les persones autoritzades.

4. Als fitxers no automatitzats de nivell mitjà se'ls hauran d'aplicar les mesures relacionades amb:

    a. Mesures de seguretat aplicables als fitxers de nivell bàsic.
    b. Nomenament del Responsable de Seguretat: es pot anomenar un únic responsable de seguretat per a tots els fitxers/tractaments de la FUAB i/o de les institucions que dirigeix aquesta Fundació amb dades de caràcter personal o es poden nomenar diversos responsables de seguretat en funció dels sistemes de tractament. Aquest nomenament quedarà reflectit en el Document de Seguretat.
    c. Auditories: s'haurà de fer una auditoria, com a mínim, cada 2 anys, de tots aquells sistemes o instal·lacions en els que es tracten fitxers amb un nivell de

seguretat mitjà. Aquesta auditoria, pel que fa als fitxers no automatitzats, verificarà l'acompliment de les mesures que es detallen en aquest document tot dictaminant sobre la seva adequació a la normativa vigent, el que comportarà l'elaboració d'informes que identifiquin els aspectes no conformes a dret i proposin les mesures correctores que el responsable de seguretat haurà d'aplicar al respecte.

5. Als fitxers no automatitzats de nivell alt se'ls hauran d'aplicar les mesures relacionades amb:

    a. Mesures de seguretat aplicables als fitxers de nivell mitjà.
    b. Emmagatzematge de documentació: la documentació s'emmagatzemarà en armaris tancats en clau (o d'altre sistema similar).
    c. Realització de còpies: només podran fer còpies de documents que contenen dades de caràcter personal de nivell alt, aquelles persones autoritzades en el document de seguretat. Es crearà un registre i un procés d'autorització excepcional per a permetre accés puntual a aquelles persones no identificades al document de seguretat.
    d. Seguretat en els trasllats: s'adoptaran les mesures necessàries, en cada cas, per tal d'evitar l'accés i/o manipulació de la informació per part de persones no autoritzades durant el trasllat físic de la documentació. Aquesta mesura, per exemple, s'haurà de tenir en compte quan es produeixi el trasllat de la documentació a l'arxiu departamental.

6. El responsable del fitxer ha de facilitar el procés de destrucció de qualsevol paper que contingui dades de caràcter personal, mitjançant la instal·lació de màquines trituradores o de contenidors específics.

CAPÍTOL V. DRETS DE LES PERSONES INTERESSADES: ACCÉS, CANCEL·LACIÓ, RECTIFICACIÓ I OPOSICIÓ

SECCIÓ PRIMERA. DISPOSICIONS GENERALS

Article 25. Consideracions generals

1. Els drets d'accés, rectificació, cancel·lació i oposició són personalíssims i, en conseqüència, hauran de ser exercits directament per la persona interessada titular de les dades. Així, no seran ateses sol·licituds per a l'exercici d'aquests drets quan es realitzin a través d'una tercera persona o per qualsevol mitjà que no permeti la identificació inequívoca de la persona interessada.

2. No obstant el que preveu l'apartat anterior, els drets esmentats podran exercir-se per la persona interessada a través del seu representant legal en els supòsits d'incapacitat o minoria d'edat.

Article 26. Legitimació

1. Els drets d'accés, rectificació, cancel·lació i oposició seran exercits per la persona interessada mitjançant escrit dirigit a la institució corresponent.

2. L'encarregat del tractament haurà d'adoptar les mesures necessàries per assegurar que el personal al seu servei que tingui accés a dades de caràcter personal pugui informar a les persones interessades del procediment a seguir per a l'exercici dels drets d'accés, rectificació, cancel·lació i oposició.

Article 27. Documentació necessària

1. L'escrit de sol·licitud de l'exercici dels drets d'accés, rectificació, cancel·lació o oposició haurà de contenir les dades identificatives de la persona interessada, i anirà acompanyat de còpia del document oficial que l'identifiqui.

2. Quan la sol·licitud es realitzi a través de persona apoderada, caldrà fer-hi constar les dades del representant, el seu document d'identitat i l'acreditació de la seva condició.

3. La persona interessada o qui la representi, determinarà la petició en què es concreta la sol·licitud i assenyalarà un domicili als efectes de notificacions.

Article 28. Resolució

Les resolucions relatives a les sol·licituds d'accés, rectificació, cancel·lació i oposició seran dictades pel director general corresponent, previ informe i proposta de la Direcció Jurídica i de RRHH de la FUAB.
Les sol·licituds d'accés seran resoltes en el termini màxim d'un mes a comptar de l'endemà de la data en què tingui entrada la sol·licitud corresponent a la Direcció Jurídica i de RRHH de la FUAB.

En el supòsit que fos necessària la millora de la sol·licitud, el termini expressat en l'apartat anterior quedarà interromput fins que la persona interessada presenti la documentació o les al·legacions complementàries.

Si la institució corresponent no té dades de caràcter personal de la persona sol·licitant, l'hi farà saber igualment en el mateix termini d'un mes.

SECCIÓ SEGONA. DRET D'ACCÉS

Article 29. Consideracions generals

1. Les persones interessades tenen dret a sol·licitar i a obtenir informació de les seves dades de caràcter personal incloses en els fitxers de la FUAB i/o en els de les empreses que dirigeix aquesta Fundació, sigui quina sigui la seva modalitat de creació, organització o emmagatzematge.

2. El dret d'accés podrà ser exercit per la persona interessada en intervals no inferiors a dotze mesos, llevat que s'acrediti l'existència de motius legítims que justifiquin un interval inferior.

Article 30. Sistemes d'accés

1. La persona interessada, a l'hora de formular la seva sol·licitud i sempre que la configuració o la implantació material del fitxer ho permeti, haurà d'optar per algun dels sistemes de consulta següents:

   - Visualització en pantalla.
   - Escrit o còpia a enviar per correu.

2. Sense perjudici del que preveu l'apartat anterior, la Fundació UAB i/o les empreses que dirigeix aquesta Fundació podran determinar el sistema de consulta que menys pertorbi el funcionament normal dels seus serveis, i ho comunicarà a la persona interessada amb la motivació corresponent.

Article 31. Constància de l'exercici dels drets

1. La institució corresponent deixarà constància de l'exercici del dret d'accés per part de les persones interessades.

2. En el supòsit que el dret d'accés es realitzi mitjançant la visualització de la pantalla, es guardarà una impressió de la pantalla consultada que serà firmada per la persona interessada.

3. Les comunicacions escrites es realitzaran mitjançant correu certificat amb avís de rebuda, o per qualsevol altre mitjà que en garanteixi la recepció per part de la persona interessada.

4. La persona responsable de cada institució vetllarà perquè el seu personal que tingui accés a les dades disposi dels mitjans necessaris per poder fer efectius els drets dels interessats.

Article 32. Consideracions generals

1. Les persones interessades, en el supòsit que les seves dades de caràcter personal siguin inexactes, incompletes, inadequades o excessives, podran sol·licitar que es rectifiquin o, si escau, que es cancel·lin.

2. Així mateix, les persones interessades podran oposar-se al tractament de les seves dades de caràcter personal quan hi hagi motius fundats i legítims relatius a una situació personal concreta.

SECCIÓ TERCERA. DRETS DE RECTIFICACIÓ, CANCEL·LACIÓ I OPOSICIÓ

Article 33. Sol·licituds

1. La sol·licitud de rectificació haurà d'indicar la dada que es considera errònia i la correcció que es proposa, acompanyada de la documentació acreditativa corresponent, llevat que la rectificació depengui exclusivament del consentiment de la persona interessada. En cas que no disposi de dades de caràcter personal de l'afectat, igualment l'hi ha de comunicar en el termini de 10 dies.

2. En la sol·licitud de cancel·lació, l'interessat ha d'indicar a quines dades es refereix, i ha d'aportar a aquest efecte la documentació que ho justifiqui, si s'escau. En cas que no disposi de dades de caràcter personal de l'afectat, igualment l'hi ha de comunicar en el termini de 10 dies.

3. Si les dades rectificades o cancel·lades han estat cedides prèviament, el responsable del fitxer ha de comunicar-ne la rectificació o cancel·lació efectuada al cessionari, en un termini idèntic, perquè el cessionari, també en el termini de deu dies comptats des de la recepció de la dita comunicació, així mateix, rectifiqui o cancel·li les dades.

4. La sol·licitud d'oposició haurà d'especificar el supòsit legítim i la situació personal concreta que, a criteri de la persona interessada, la justifiquen.

Article 34. Límits

1. La cancel·lació no es durà a terme quan pugui perjudicar els drets de la persona interessada o de terceres persones, o quan hi hagi obligació legal de conservar les dades.

2. El dret d'oposició només podrà ser exercit en els supòsits en què el consentiment de la persona afectada no sigui necessari per al tractament de les dades i sempre que la llei no disposi altrament.

Article 35. Efectes de la cancel·lació

1. La cancel·lació exigeix l'eliminació física de la dada, sense que sigui suficient una marca lògica ni la inclusió de la dada esborrada en un fitxer alternatiu de dades cancel·lades.

2. En el supòsit que, per raons tècniques, no sigui possible l'eliminació física de la dada, la persona responsable del tractament procedirà al bloqueig de la dada, per tal d'impedir-ne l'accés o l'ús.

CAPÍTOL VI. DISPOSICIONS FINALS

Primera. Interpretació

Qualsevol dubte en l'aplicació d'aquest reglament intern o en les disposicions legals vigents en matèria de protecció de dades personals serà tramesa per escrit a la Direcció Jurídica i de RRHH de la FUAB.

Apartat 2 del Document de Seguretat

MESURES, NORMES, PROCEDIMENTS I REGLES DE SEGURETAT APLICABLES A FITXERS I TRACTAMENTS AUTOMATITZATS

Per tal de complir el que disposa el Títol VIII Capítol III del RLOPD en relació a les mesures de seguretat aplicables els fitxers i tractaments automatitzats, la Fundación Wassu (WASSU) ha establert les mesures de seguretat següents, que hauran de ser conegudes, acceptades, respectades i aplicades per tot el personal de la WASSU.

PLA DE SEGURETAT

El pla de seguretat contempla les mesures, les normes i els procediments recollits en el present document, amb la finalitat de garantir el nivell de seguretat exigit per la LOPD i el RLOPD.

Per tal d'assolir aquest objectiu s'inclouen als següents apartats, un conjunt de mesures que afecten directament la seguretat dels fitxers de dades i tractaments automatitzats i no automatitzats.

IDENTIFICACIÓ I AUTENTICACIÓ

Les normes següents regulen els procediments d'identificació i d'autenticació, d'acord amb l'article 93 del RLOPD pels fitxers automatitzats, sense perjudici de l'aplicació del procediment per a l'assignació i la gestió de claus de pas associades a cada usuari amb accés als sistemes d'informació de la WASSU.

1. La WASSU custodia i actualitza la relació de tots els usuaris de la xarxa que tenen accés autoritzat als seus sistemes d'informació, així com la relació d'usuaris amb accés als arxius protegits. És competència seva l'assignació de contrasenyes, així com que la custodia es realitzi amb garanties de confidencialitat i d'integritat.
2. Els identificadors de l'usuari i de contrasenya assignats a cada usuari de la xarxa corporativa de la WASSU, són personals i intransferibles, i cada usuari és l'únic responsable de les conseqüències derivades de fer-ne mal ús, de divulgar-los o de perdre'ls. Quan un usuari tingui la sospita que algú coneix la seva contrasenya, serà responsable de sol·licitar-ne el canvi.
3. Existeix un bloqueig d'usuari si aquest intenta accedir reiteradament al sistema sense disposar-ne d'accés (3 vegades com a màxim).

CONTROL D'ACCÉS I CONFIDENCIALITAT DE LA INFORMACIÓ

Per tenir accés a la xarxa corporativa s'han de seguir una sèrie de pautes i normes de comportament que són les següents:

1. Tota la informació emmagatzemada a la xarxa corporativa, de forma estàtica o que circuli en forma de missatges de correu electrònic, és propietat de la WASSU i té caràcter confidencial.
2. Es considera informació especialment reservada els procediments, les metodologies, les bases de dades i qualsevol altre material de caràcter estratègic i confidencial que formi part de l'activitat de la WASSU.
3. Els usuaris tindran accés autoritzat únicament a aquelles dades i recursos que siguin necessaris per dur a terme les seves funcions.
4. Només el personal autoritzat podrà concedir, modificar o anul·lar l'accés a les dades i recursos, en funció dels criteris establerts pel responsable del fitxer.

GESTIÓ DE SUPORTS

En relació a la gestió de suports s'ha d'observar el següent:

1. Existeix un procediment d'identificació, inventari i custòdia de suports informàtics amb dades de caràcter personal. L'objectiu d'aquest procediment és permetre identificar el tipus d'informació que contenen els suports, inventariar-los i emmagatzemar-los en un lloc d'accés restringit al personal autoritzat.
2. Únicament el responsable del fitxer podrà autoritzar la sortida de suports informàtics que continguin dades personals fora dels seus locals habituals.

ÚS DE CORREU ELECTRÒNIC

1. Els ordinadors de l'oficina i, en general, tot el sistema informàtic utilitzat per cada usuari, són propietat de la WASSU.
2. Cap missatge de correu electrònic serà considerat privat, considerant correu electrònic tant el correu intern, entre terminals de la xarxa corporativa, com extern dirigit a altres xarxes públiques o privades i, en especial, Internet.
3. La WASSU es reserva el dret de revisar, sense avís previ, els missatges de correu electrònic dels usuaris dels ordinadors de la seva propietat, amb la finalitat de verificar el compliment d'aquestes normes i prevenir activitats que puguin afectar a la WASSU com a responsable civil.
4. Qualsevol fitxer introduït en els ordinadors de la WASSU mitjançant missatges de correu electrònic provinents de xarxes internes ha de complir els requisits establerts en aquestes normes i, en especial, les que fan referència a la propietat intel·lectual i el control de virus.
5. L'usuari és completament responsable de totes les activitats realitzades amb el seu compte d'accés i la seva bústia associada a la WASSU.
6. És una falta greu facilitar i/o oferir a tercers el compte i la bústia personals.
7. S'ha de conèixer la diferència entre utilitzar les adreces de correu electrònic de la WASSU o altres adreces ofertes per altres proveïdors d'accés a Internet. Per a temes de caràcter aliè al treball de la WASSU idealment s'hauria de treballar amb adreces de proveïdors externs, mai des de la WASSU ni amb els comptes que en dóna.
8. Correu personal: els serveis de correu electrònic subministrats per la WASSU poden fer-se servir de forma accidental per a temes personals, excepte, si interfereixen amb el rendiment del propi servei, interfereixen en les tasques pròpies dels gestors del servei, es fan servir per a propòsits financers o comercials, o suposen un cost elevat per a la Fundació.
9. L'usuari de correu electrònic no practicarà cap de les tècniques que es coneixen com a Tècniques d'Abús en el Correu Electrònic i que inclouen:
    - ✓ Difusió de continguts inadequats, especialment continguts il·legals per naturalesa o que constitueixin complicitat amb delictes. Per exemple: apologia del terrorisme, programes pirates, pornografia infantil, amenaces, estafes, esquemes d'enriquiment piramidal, virus o codis hostils en general. També són continguts inadequats els que s'envien a grups temàtics fora de context i la propagació de cartes encadenades.
    - ✓ No és correcte enviar correu a persones que no desitgen rebre'l. Si es demana a un usuari que aturi aquesta pràctica, aquest ho ha de fer. Si la WASSU rep queixes, denúncies o reclamacions per aquestes pràctiques, es prendran les mesures que determina la Normativa de Seguretat.

- ✓ També es consideren continguts inadequats els que s'enviïn a grups de discussió (llistes de distribució, grups de notícies o butlletins electrònics) que comprometin la reputació de la WASSU.
- ✓ Difusió mitjançant canals no autoritzats: ús no autoritzat d'un servidor aliè per reenviar correu propi. Això és d'aplicació fins i tot per als missatges que en sí són legítims, en el cas de que es facin servir recursos aliens sense consentiment dels afectats.
- ✓ Difusió d'informació no autoritzada: utilitzar el servei per enviar publicitat o qualsevol tipus de correu no sol·licitat o aliè a la WASSU, especialment quan aquesta difusió és massiva.
- ✓ Atacs amb l'objecte d'impossibilitar o dificultar el servei, tant dirigits a un usuari com al propi sistema de correu. Es poden considerar com una inversió del concepte de difusió massiva (1→n), en el sentit que són atacs tipus (n→1).
- ✓ Subscripció indiscriminada a llistes de correu i subscripció a tercers: una versió de l'atac anterior.
- ✓ Falsificar o modificar les capçaleres de correu electrònic.

ACCÉS A INTERNET

1. L'ús dels sistemes informàtics dirigits per la WASSU, per accedir a xarxes públiques com Internet es limitarà als temes directament relacionats amb l'activitat de la WASSU i amb les tasques de l'usuari en el seu lloc de treball. Actualment, tots els usuaris tenen accés a Internet i no existeix cap restricció d'accés.
2. L'accés a aplicacions de debat en temps real (chat / IRC, Messenger, etc) és especialment perillós, ja que, facilita la instal·lació d'utilitats que permeten accés no autoritzat al sistema. Per aquest motiu la WASSU es reserva el dret d'impossibilitar l'ús d'aquestes eines per raons de seguretat.
3. L'accés a pàgines web (www), grups de notícies (Newsgroups) i altres utilitats com FTP, Telnet, etc, es podrà limitar en qualsevol instant per evitar la descàrrega de programes que puguin malmetre el sistema.
4. La WASSU es reserva el dret de monitoritzar i verificar, de forma aleatòria i sense avís previ, els *logs* d'accés a Internet dels diferents usuaris des del seu ordinador de treball, amb la finalitat de prevenir l'ús fraudulent, il·legal, abusiu o no autoritzat d'Internet. Aquesta monitorització pot incloure la revisió dels registres que mostren els fitxers carregats i accedits, les pàgines web visitades i els usuaris que han realitzat aquestes accions, així com el moment en què s'han produït.
5. Qualsevol persona que accedeix a Internet mitjançant la xarxa de la WASSU accepta aquesta monitorització així com les normes establertes, i assumeix les accions disciplinàries per incompliment d'aquestes normes.
6. Es prohibeix la descàrrega mitjançant Internet de software d'origen desconegut o propietat de tercers en els sistemes de la WASSU, a excepció de l'existència d'autorització prèvia de la Direcció de la mateixa WASSU.

PROPIETAT INTEL·LECTUAL I INDUSTRIAL

Queda estrictament prohibit l'ús de programes informàtics sense la corresponent llicència, així com l'ús, reproducció, transformació o comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual i industrial.

Les utilitzacions il·lícites que es facin de programes informàtics sense la corresponent llicència serà assumit per l'usuari. La WASSU podrà emprendre les accions legals oportunes que calguin, a fi efecte, de depurar les responsabilitats de les persones autores dels fets.

FITXERS TEMPORALS

Durant el tractament dels fitxers, pot ser necessari crear fitxers temporals que facilitin el treball amb les dades de caràcter personal.

Els requisits imprescindibles per poder extreure les dades dels fitxers o bases de dades preexistents i dipositar-les en altres fitxers de nova creació de caràcter temporal, són les següents:

1. Que el sistema informàtic on s'emmagatzemin els nous fitxers temporals compleixi amb les mateixes mesures de seguretat que les establertes en el present document. Si són creats en format de paper cal emmagatzemar-los correctament quan no siguin necessaris per a la finalitat per la que es van crear.
2. Que el fitxer temporal sigui eliminat quan ja no sigui necessari per a la finalitat per la qual es va crear. En cas de no complir els requisits anteriors el fitxer temporal no es podrà crear, a no ser que existeixi una autorització del responsable de seguretat. En aquest cas, els fitxers temporals resultants d'una extracció hauran de ser destruïts després del seu ús.

Apartat 3 del Document de Seguretat

FUNCIONS I OBLIGACIONS DEL PERSONAL

Per tal de complir el que disposa l'article 89 i següents del RLOPD, la FUAB ha establert les mesures de seguretat següents, que hauran de ser conegudes, acceptades i respectades per tot el personal de la FUAB i/o de les institucions que dirigeix aquesta Fundació.

DE TOT EL PERSONAL

Identificadors d'usuari i contrasenyes

1. Tots els usuaris han d'accedir al sistema informàtic de la WASSU utilitzant un nom d'usuari i una contrasenya que els identifiqui i els n'autoritzi l'accés.
2. Queda prohibit comunicar a qualsevol altra persona el nom d'usuari i la clau d'accés. Si l'usuari sospita que algú coneix el seu identificador i clau de pas, haurà de canviar la seva clau de pas per garantir la seva confidencialitat. En cas d'una baixa o absència temporal de l'usuari, el responsable de la WASSU podrà sol·licitar, en cas justificat i sota la seva responsabilitat, el canvi de la clau de pas d'aquest usuari, per tal de poder accedir als recursos de la seva propietat durant la seva absència.
3. L'usuari està obligat a utilitzar la xarxa i els sistemes d'informació sense caure en activitats que puguin ser considerades il·lícites o il·legals, que infringeixin els drets de la WASSU, o de tercers, o que puguin atemptar contra la moral o les bones formes de treball de les xarxes telemàtiques.
4. Estan expressament prohibides les activitats següents:
   - ✓ Compartir o facilitar l'identificador de l'usuari i la clau de pas per accedir als sistemes d'informació de la WASSU a cap altre persona física o jurídica, inclòs el personal de la pròpia empresa. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable dels actes de la persona física o jurídica que utilitzi de forma no autoritzada els seu identificador d'usuari.
   - ✓ Intentar distorsionar o falsejar les dades de les aplicacions.
   - ✓ Intentar desxifrar les claus, sistemes o algoritmes de xifrat, i qualsevol altre element de seguretat que intervingui en els processos telemàtics de la WASSU.
   - ✓ Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris. Aquesta acció pot ser considerada un delicte d'interceptació de les telecomunicacions, descrit a l'article 197 del Codi Penal.
   - ✓ Utilitzar el sistema per intentar accedir a les àrees restringides dels sistemes informàtics de la WASSU o de tercers.
   - ✓ Intentar augmentar el nivell de privilegis d'un usuari en el sistema.

Utilització dels sistemes informàtics

Els usuaris que utilitzin Internet han de fer un bon ús de la xarxa, per tal d'evitar tràfic innecessari en la xarxa o interferències en el treball d'altres usuaris, o amb altres xarxes associades i els serveis que aquestes ofereixen.

En concret, estan especialment prohibides les activitats següents:

1. Destruir, manipular, inutilitzar o qualsevol altra forma de malmetre dades, programes, i documents electrònics de la WASSU o de tercers. Aquests actes poden ser un delicte, descrit a l'article 264.2 del Codi Penal.
2. Realitzar accions per malmetre, interrompre o generar errors als sistemes de la WASSU.
3. Enviar missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitàries sense el consentiment del destinatari (*spam*).
4. Introduir voluntàriament programes, virus, macros, *applets*, controls Active X o qualsevol altre dispositiu lògic o seqüència de caràcters que produeixin qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o de tercers. L'usuari tindrà l'obligació d'utilitzar els programes antivirus corporatius i les seves actualitzacions per prevenir l'entrada al sistema de qualsevol element destinat a destruir o corrompre dades.
5. Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per la WASSU, o qualsevol altre tipus d'obra o material amb drets de propietat intel·lectual o industrial per part de tercers, quan no es disposi de la corresponent autorització.
6. Instal·lar còpies il·legals de qualsevol programa, inclosos els corporatius.
7. Desinstal·lar qualsevol dels programes instal·lats legalment.
8. Utilitzar els recursos telemàtics de la WASSU, inclòs l'accés a la xarxa d'Internet, per activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.
9. Introduir en el seu ordinador de treball continguts immorals o ofensius i, en general, sense cap utilitat per a les finalitats pròpies de la WASSU.
10. Enviar o reenviar missatges en cadena o de tipus piramidal.
11. L'ús de correu electrònic, Internet i propietat intel·lectual i industrial ve regulat per les normes i procediments especificats en el punt 2 d'aquest document.
12. Fer un mal ús de la xarxa Wireless. Els usuaris que en facin es posaran a la llista negra de la passarel·la, en els terminis que es determinin per a l'aplicació de les sancions que contempla la normativa de seguretat de les empreses de l'entorn FUAB. Les llistes negres poden configurar-se de manera que:

- ✓ No permetin accedir a la xarxa.
- ✓ Permetin només accedir a la xarxa sense sortir de la WASSU.
- ✓ Bloquegin l'accés a determinats serveis o servidors.

<u>Confidencialitat de la informació</u>

1. Queda prohibit enviar informació confidencial de la WASSU a l'exterior, bé mitjançant suports materials o a través de qualsevol mitjà de comunicació, així com la simple visualització o accés (1).

[1] Aquesta prohibició no s'aplicarà en l'enviament d'informació confidencial a empreses, professionals o associacions subcontractades, sempre que en els contractes establerts amb aquestes empreses, es contempli el que s'estableix en l'article 12 de la Llei de Protecció de Dades de caràcter personal.

2. Els usuaris dels sistemes d'informació han de guardar, per temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni mitjançant terceres persones o empreses, dades, documents, metodologies, claus, anàlisis, programes i tota informació a la que tinguin accés durant la seva relació laboral amb la WASSU, tant en suport material com electrònic. Aquesta obligació continuarà vigent després de l'extinció del contracte laboral (article 10 LOPD).
3. Cap col·laborador pot apropiar-se de cap material o informació propietat de la WASSU per fer ús diferent de les seves responsabilitats, tant ara com en el futur.
4. En cas que, per motius directament relacionats amb el lloc de treball, l'empleat entri en possessió d'informació confidencial en qualsevol format o suport, ha d'assumir que aquesta possessió és estrictament temporal, amb l'obligació de mantenir-la en secret i sense que això li doni cap dret de possessió, titularitat o de fer còpia d'aquesta informació. De la mateixa manera, el treballador ha de tornar els citats materials a la WASSU, immediatament després de la finalització de les tasques que van originar el seu ús temporal i, en qualsevol cas, en el moment de la finalització de la relació laboral. La utilització continuada d'aquesta informació, en qualsevol format o suport de forma diferent a la pactada i sense coneixement de la WASSU no suposarà, en cap cas, una modificació d'aquesta clàusula. L'incompliment d'aquesta obligació es pot considerar un delicte de revelació d'informació, previst a l'article 197 i següents del Codi Penal, i donarà dret a la WASSU a exigir responsabilitats a l'usuari.

Incidències

1. Tot el personal de la WASSU té l'obligació de comunicar al responsable de seguretat qualsevol incidència que es produeixi en els sistemes d'informació als que tenen accés.
2. Per incidència entendrem qualsevol anomalia que afecti o que pugui afectar la seguretat de les dades o els sistemes de tractament dels fitxers que continguin dades de persones físiques.
3. La comunicació de la incidència ha de realitzar-se en un interval de temps no superior a una hora des del moment en què sigui detectada.

Protecció de dades

1. La creació, modificació o supressió dels fitxers automatitzats que continguin dades de caràcter personal ha de ser notificada a la Direcció Jurídica i de RRHH de la FUAB, que és el departament competent per fer aquesta comunicació a l'Agència Catalana de Protecció de Dades (APDCAT), segons la normativa interna de les institucions de l'entorn FUAB. També cal notificar qualsevol canvi que afecti la finalitat declarada del fitxer, el seu responsable, la seva ubicació o qualsevol altra circumstància relativa a fitxers ja registrats a l'APDCAT.
2. La WASSU notificarà als seus alumnes, proveïdors i clients en el moment de recollir les dades, a excepció que la Llei alliberi d'aquesta obligació, la següent informació:
   - ✓ L'existència del fitxer.
   - ✓ La finalitat de la recollida de dades.
   - ✓ La persona destinatària de la informació.
   - ✓ La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació o oposició.
   - ✓ La identitat i adreça del responsable del fitxer.
   - ✓ Les conseqüències de no subministrar la informació demanada i el caràcter obligatori o no de respondre a les preguntes realitzades.

3. La recollida de les dades sensibles que afectin la ideologia, l'afiliació sindical, la religió i les creences, l'origen racial, la salut i la vida sexual, requerirà el consentiment per escrit dels afectats a qui se'ls ha sol·licitat.
4. Les cessions o comunicacions de dades de caràcter personal es realitzaran d'acord amb els requisits següents (Art. 10 RLOPD):
   - ✓ Amb aprovació prèvia de la persona, a no ser que la Llei alliberi d'aquesta obligació.
   - ✓ Complint finalitats directament relacionades amb les funcions pròpies de la WASSU.
5. La creació d'un fitxer en l'àmbit local (en el disc dur de l'ordinador) suposarà la total assumpció de responsabilitat per part de l'usuari davant la implantació i el control de les mesures tècniques i controls de seguretat establerts per la legalitat vigent en aquesta matèria.

Article 5 del Document de Seguretat

PROCEDIMENT DE REGISTRE, NOTIFICACIÓ I RESPOSTA DE LES INCIDÈNCIES

Una incidència és qualsevol esdeveniment que pugui produir-se esporàdicament i que pugui suposar un perill per a la seguretat dels fitxers, entesa sota les seves tres vessants de confidencialitat, integritat i disponibilitat de les dades.

Mantenir un registre de les incidències que comprometin la seguretat dels fitxers és una eina imprescindible per a la prevenció de possibles atacs a aquesta seguretat, així com per a la persecució dels responsables dels mateixos.

1. El Responsable de Seguretat dels fitxers habilitarà un Registre d'Incidències que estarà a disposició de tots els usuaris i Administradors dels fitxers amb la finalitat de què allà es registri qualsevol incidència que pugui suposar un perill per a la seguretat dels mateixos.

2. Qualsevol usuari que tingui coneixement d'una incidència és responsable del registre de la mateixa en el Registre d'Incidències dels fitxers o, si s'escau, de la comunicació per escrit al Responsable de Seguretat o al Responsable dels Fitxers.

3. El coneixement i la no notificació o registre d'una incidència, per part d'un usuari, serà considerat com una falta contra la seguretat dels fitxers per part d'aquest usuari.

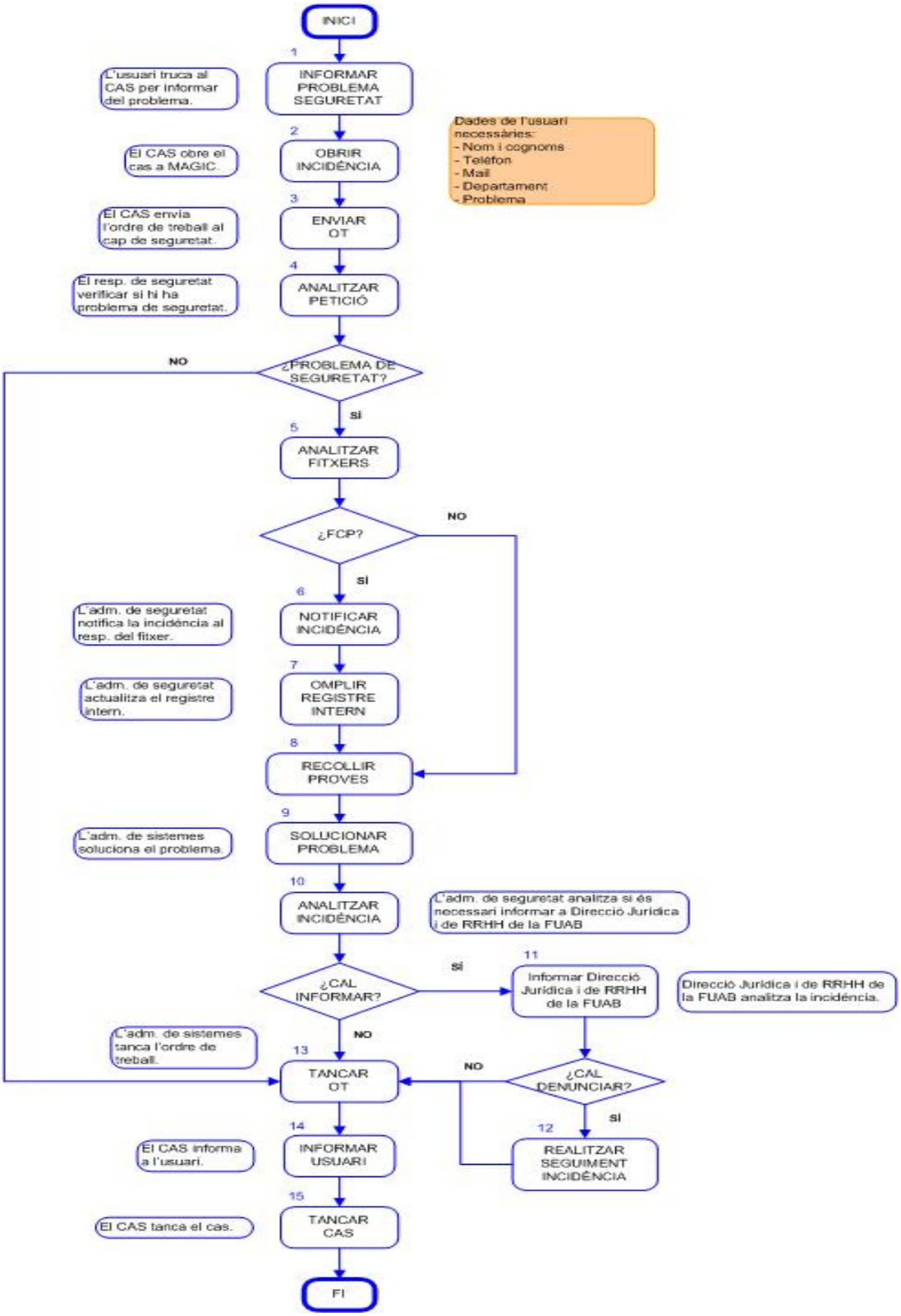
4. La notificació o registre d'una incidència haurà de constar, com a mínim, de les següents dades: tipus d'incidència, data i hora en què es va produir o detectar, persona que realitza la notificació, persona a qui es comunica, efectes que poden derivar-se i mesures correctores aplicades.

TIPOLOGIA DE LES INCIDÈNCIES

Tot i que la tipologia d'incidències pot ser molt variada, a continuació es recullen algunes de les que poden afectar a la seguretat de les dades de caràcter personal:

TIPUS	DESCRIPCIÓ	EXEMPLE
Accés denegat	Es produirà quan després d'haver introduït els *login* i *password* de l'usuari, no li sigui permès accedir al sistema.	Quan es detecta un nombre d'intents d'accés a un sistema superior a l'establert.
Accés no autoritzat.	Es produirà quan s'accedeixi a l'equip o als serveis pels quals no es té autorització.	Accés a l'equip o al correu d'un company amb el seu *login*
Atac extern	Es produirà quan el sistema sigui atacat des de l'exterior.	Virus, troians, intrusió d'accés, etc.
Pèrdua d'informació.	Es produirà quan es detecti una pèrdua de dades després d'un problema en el sistema.	Avaria de discs, problemes en recuperar una còpia de seguretat,...
Alteració no autoritzada de les dades	Es produirà quan es modifiquin dades sense el consentiment del propietari i del responsable de fitxer.	Actuacions malintencionades de persones amb accessos no autoritzats.
Sostracció o pèrdua de hardware.	Es produirà quan es perdin o siguin sostrets consentiment parts o equips que continguin dades de caràcter personal.	Robatoris o pèrdues de suports.
Recuperació de fitxers	Es produirà quan, després de la pèrdua d'algun fitxer, sigui necessària la recuperació de les dades d'una còpia de seguretat.	Danys en fitxers, impossibilitat de lectures...
Infecció Vírica	Es produirà quan un PC no disposi de protecció antivírica o aquesta no estigui actualitzada.	Danys en fitxers i sistemes.

Esquema del procés de gestió de les incidències:



REGISTRE D'INCIDÈNCIES

Per cada incidència que es produeixi es generarà un registre d'incidències en el qual s'inclouran, entre d'altres, les dades següents:

- ✓ Número d'incidència.
- ✓ Tipus d'incidència.
- ✓ Descripció detallada de la incidència.
- ✓ Data i hora en què s'ha detectat la incidència.
- ✓ Persona que notifica la incidència.
- ✓ Persona a la que se li comunica la incidència.
- ✓ Efectes derivats i solució adoptada.

A més de les dades anteriors, quan sigui necessària una recuperació de dades de nivell mitjà o alt, caldrà incloure en el registre d'incidències la informació següent:

- ✓ Procediment de recuperació de dades.
- ✓ Persona que va executar el procediment.
- ✓ Dades restaurades.
- ✓ Dades gravades manualment durant la recuperació manual.

En aquests casos, i en funció del nivell de seguretat amb el que tractem, també serà necessària l'autorització per escrit del responsable del fitxer.

MODEL PER AL REGISTRE D'INCIDÈNCIES

Per cada incidència que es detecti, es generarà un registre d'incidències utilitzant els dos models que conté aquest document, un per a fitxers de nivell bàsic (model 8), i un altre per a fitxers de nivells mitjà i alt (model 9).

ANNEXOS: MODELS DE DOCUMENTS

INFORMACIÓ A L'INTERESSAT

Les dades personals que faciliteu passaran a formar part del fitxer (nom del fitxer) de (nom de la institució) amb la finalitat de (...*). Podeu exercir els drets d'accés, rectificació, cancel·lació i oposició davant (nom, adreça postal, adreça electrònica i telèfon de la institució) mitjançant un escrit i adjuntant fotocòpia del Document d'Identitat.

(*)mantenir la relació contractual amb el client, de realitzar estudis estadístics i d'enviar publicitat relativa a (nom de la institució)

(*) mantenir i gestionar la relació amb l'alumne i de trametre informació tècnica, operativa, publicitària o promocional de ...

Si teniu previst fer cessions de dades a altres empreses del grup, haureu d'incloure el paràgraf següent:

Les dades podran ser cedides a altres empreses o institucions vinculades a la Universitat Autònoma de Barcelona o a la Fundació Universitat Autònoma de Barcelona per a les mateixes finalitats.

EXERCICI DEL DRET D'ACCÉS A LES DADES DE CARÀCTER PERSONAL

Dades del Responsable del Fitxer o Tractament públic
Nom, càrrec o òrgan administratiu
Adreça
Localitat
(si no coneix l'adreça pot sol·licitar-la al Registre de Protecció de Dades de Catalunya d'acord amb l'article 7 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades)

Dades del Sol·licitant
Nom
DNI *(cal adjuntar fotocòpia)*
Adreça

Assumpte:
Sol·licitud d'informació sobre les dades personals incloses en un fitxer o tractament

D'acord amb allò establert a l'article 15 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, sol·licito que m'indiqui si disposen d'informació sobre les meves dades personals incloses en els seus fitxers.

En cas afirmatiu, demano que m'adrecin aquesta informació de forma clara i intel·ligible, així com les dades resultants de qualsevol elaboració, procés o tractament, l'origen de les dades, els cessionaris i els usos i finalitats per a les quals es van emmagatzemar.

En cas de no atendre aquesta petició d'accés, en el termini d'un mes, s'entendrà que és desestimada, per la qual cosa es podrà interposar l'oportuna reclamació a l'Agència Catalana de Protecció de Dades per iniciar el procediment de tutela dels drets d'acord amb l'article 7.2 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

(Localitat, Data)

(signatura del sol·licitant)

EXERCICI DEL DRET DE RECTIFICACIÓ DE DADES DE CARÀCTER PERSONAL

Dades del Responsable del Fitxer o Tractament públics
Nom, càrrec o òrgan administratiu
Adreça
Localitat
(si no coneix l'adreça pot sol·licitar-la al Registre de Protecció de Dades de Catalunya d'acord amb l'article 7 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de protecció de Dades)

Dades del Sol·licitant

Nom
DNI *(cal adjuntar fotocòpia)*
Adreça

Assumpte:
Sol·licitud de rectificació sobre les dades personals incloses en un fitxer o tractament

D'acord amb allò establert a l'article 16 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, sol·licito que es corregeixin les dades inexactes que es contenen als seus fitxers, que apareixen relacionades a continuació i de les quals n'adjunto la documentació acreditativa:

Dada incorrecta **Dada correcta** **Document acreditatiu**

En el termini de deu dies des de la recepció d'aquesta sol·licitud s'haurà de fer efectiva aquesta correcció, per la qual cosa sol·licito que se'm comuniqui la rectificació una vegada realitzada o bé el motiu pel qual el responsable del fitxer considera que l'esmena no procedeix.

En cas de no atendre aquesta petició es podrà interposar l'oportuna reclamació a l'Agència Catalana de Protecció de Dades per iniciar el procediment de tutela dels drets d'acord amb l'article 7.2 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

(Localitat, Data)

(signatura del sol·licitant)

EXERCICI DEL DRET DE CANCEL·LACIÓ DE DADES DE CARÀCTER PERSONAL

Dades del Responsable del Fitxer o Tractament públic
Nom, càrrec o òrgan administratiu
Adreça
Localitat
(si no coneix l'adreça pot sol·licitar-la al Registre de Protecció de Dades de Catalunya d'acord amb l'article 7 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades)

Dades del Sol·licitant
Nom
DNI *(cal adjuntar fotocòpia)*
Adreça

Assumpte:
Sol·licitud de cancel·lació sobre les dades personals incloses en un fitxer o tractament

D'acord amb allò establert a l'article 16 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, sol·licito que es cancel·lin les meves dades personals que es continguin en els vostres fitxers.

En el termini de deu dies des de la recepció d'aquesta sol·licitud s'haurà de fer efectiva aquesta cancel·lació, per la qual cosa sol·licito que se'm comuniqui la realització d'aquesta o bé el motiu pel qual el responsable del fitxer considera que no procedeix.

En cas de no atendre aquesta petició es podrà interposar l'oportuna reclamació a l'Agència Catalana de Protecció de Dades per iniciar el procediment de tutela dels drets d'acord amb l'article 7.2 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

(Localitat, Data)

(signatura del sol·licitant)

EXERCICI DEL DRET D'OPOSICIÓ AL TRACTAMENT DE DADES DE CARÀCTER PERSONAL

Dades del Responsable del Fitxer o Tractament públic
Nom, càrrec o òrgan administratiu
Adreça
Localitat
(si no coneix l'adreça pot sol·licitar-la al Registre de Protecció de Dades de Catalunya d'acord amb l'article 7 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades)

Dades del Sol·licitant
Nom
DNI *(cal adjuntar fotocòpia)*
Adreça

Assumpte:
Oposició al tractament de dades personals en relació amb un fitxer o tractament

D'acord amb allò establert a l'article 6.4 i 17 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, m'oposo al tractament de les meves dades personals en base als motius següents:

(el sol·licitant haurà d'enumerar o exposar els motius fonamentats i legítims, en relació amb una concreta situació, pels quals s'oposa al tractament de les seves dades personals)

1-
2-
(…)

A fi d'acreditar els motius fonamentats i legítims per oposar-me al tractament aporto la documentació justificativa següent:

1-
2-
(…)

En cas de no atendre aquesta petició es podrà interposar l'oportuna reclamació a l'Agència Catalana de Protecció de Dades per iniciar el procediment de tutela dels drets d'acord amb l'article 7.2 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

(Localitat, Data)

(signatura del sol·licitant)

NOTIFICACIÓ D'INCIDÈNCIA GENERAL

Incidència número			
Data de notificació		Data de la incidència	
Tipus d'incidència			
Descripció detallada de la incidència			
Persones a qui es comunica			
Nom:	Càrrec:		
Nom:	Càrrec:		
Nom:	Càrrec:		
Efectes que pot produir			
Persona que realitza la comunicació		Signatura del/s Responsable/s del fitxer	
Signatura		Signatura	

NOTIFICACIÓ D'INCIDÈNCIA DE RECUPERACIÓ DE DADES

Incidència número			
Data de notificació		Data de la incidència	
Tipus d'incidència			
Descripció detallada de la incidència			
Fitxer/s: Dades afectades:			
Persones a qui es comunica			
Nom:	Càrrec:		
Nom:	Càrrec:		
Nom:	Càrrec:		
Procediment de recuperació realitzat			
Procediment Automatitzat: Procediment Manual:			
Persona que realitza la comunicació		Signatura del/s Responsable/s del fitxer	
Signatura		Signatura	