*Acord del Consell de Govern de 19 de gener de 2006*

Universitat Autònoma de Barcelona

# DOCUMENT DE SEGURETAT DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

# FULL DE CONTROL DOCUMENTAL

| VERSIÓ | DATA | CANVIS REALITZATS | RESPONSABLE |
|---|---|---|---|
| 1.0 | 19/06/2002 | DOCUMENT INICIAL | AUSEBA |
| 2.0 | 31/05/2005 | DOCUMENT UNIFICAT | UAB |
| | | | |
| | | | |

# ÍNDEX

# ÍNDEX

# INTRODUCCIÓ

# 1. INTRODUCCIÓ

El present Document respon a la necessitat de la **UNIVERSITAT AUTÒNOMA DE BARCELONA** de complir amb els requisits expressats en el Reglament de Mesures de Seguretat, expressat en el Reial Decret 994/1999 d'11 de juny de 1999 per als Fitxers Automatitzats que continguin Dades de Caràcter Personal, tant de Nivell Alt, Mitjà com Baix.

En aquest Document de Seguretat es defineixen, tant les mesures organitzatives com les tècniques que ha de complir tot el personal de l'empresa per observar un estricte compliment de la legislació vigent sobre aquest tema.

Així mateix, el seu propòsit és ajudar-nos a millorar la qualitat dels nostres serveis, oferint una major seguretat i confiança en les transaccions, garantint que complim i comprenem la legislació de protecció de dades de caràcter personal, així com l'esperit de la citada normativa en quant a garantir el dret a la intimitat de les persones relacionades amb la nostra organització.

# ÀMBIT D'APLICACIÓ DEL DOCUMENT DE SEGURETAT

# 2. ÀMBIT D'APLICACIÓ DEL DOCUMENT DE SEGURETAT

El nostre sistema de Seguretat de Dades afecta les polítiques, estructures organitzatives, responsabilitats, procediments, processos i recursos utilitzats per la **UNIVERSITAT AUTÒNOMA DE BARCELONA** per poder realitzar el seu procés productiu.

Totes les àrees de l'Organització que tenen o poden tenir relació amb Dades de Caràcter Personal, estan implicades en el compliment de la LOPD i per tant han d'ésser reflectides en aquest Document de Seguretat.

## 2.1 Àmbit Jurídic

El present Document de Seguretat s'aplicarà a tots els fitxers automatitzats de Nivells Alt, Mitjà i Baix, propietat de la **UNIVERSITAT AUTÒNOMA DE BARCELONA** .

Els fitxers automatitzats estan detallats en *l'ANNEX 1.1 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL ALT, l'ANNEX 1.2 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL MITJÀ i l'ANNEX 1.3 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL BAIX* del present Document de Seguretat.

D'igual manera, s'aplicarà a qualsevol fitxer temporal, parcial o de proves, extret dels sistemes d'informació o dels fitxers citats a l'annex.

## 2.2 Àmbit Personal

Aquest Document de Seguretat és d'obligat compliment per a tot el personal de la **UNIVERSITAT AUTÒNOMA DE BARCELONA,** ja sigui funcionari, laboral, interí, eventual o vinculat a través de qualsevol altre relació contractual, així com a qualsevol altre personal que presti els seus serveis, encara que no disposi de cap vincle contractual.

Les normes internes contingudes en el present Document s'han posat en coneixement de tot el personal de la **UNIVERSITAT AUTÒNOMA DE BARCELONA**, amb l'objecte de donar degut compliment a l'obligació continguda en l'Art. 9.2 del Reial Decret 994/1999.

## 2.3 Centres de Tractament

Els centres de tractament i procés de dades de caràcter personal inclosos dins l'àmbit d'aplicació d'aquest document estan definits a *l'ANNEX 3 – CENTRES DE TRACTAMENT*.

Els locals on s'ubiquin els ordinadors que contenen els fitxers deuen ser objecte d'especial protecció, que garanteixi la disponibilitat i confidencialitat de les dades protegides, especialment en el cas que fitxers estiguin ubicats en un servidor accedit a través de la xarxa.

Els locals hauran de disposar dels mitjans mínims de seguretat que evitin els riscos de no disponibilitat dels fitxers, que puguin produir-se a conseqüència d'incidències fortuïtes o intencionades.

## 2.4 Àmbit Material

Les presents normes de seguretat són d'aplicació als recursos informàtics de la **UNIVERSITAT AUTÒNOMA DE BARCELONA** que es descriuen a continuació:

- Servidors de dades i d'aplicacions ubicats en els centres de tractament.
- Xarxa corporativa.
- Equips de comunicacions.
- Equips de sobretaula i portàtils.
- Accés a Internet.
- Correu electrònic corporatiu.
- Centres de tractament.
- Locals.
- Sistemes informàtics o aplicacions.

A més s'inclouen tots aquells mitjans que puguin ésser suport de dades de caràcter personal afectats per la normativa sobre Seguretat de Dades:

- Suports que continguin dades de caràcter personal (discos, cintes, disquets, etc.).

- Suports amb còpies de seguretat.

# GESTIÓ GENERAL DEL PROCÉS

# 3. GESTIÓ GENERAL DEL PROCÉS

En aquest apartat s'emmarca la metodologia, les normes i procediments que regeixen a la **UNIVERSITAT AUTÒNOMA DE BARCELONA** per complir amb el Reglament de Mesures de Seguretat dels Fitxers Automatitzats i la Llei de Protecció de Dades Personals.

## 3.1 Normes

Perquè es pugui realitzar un seguiment sobre les mesures de seguretat dels fitxers automatitzats que s'ajusti a les directrius emmarcades per la legislació, s'han creat una sèrie de normes que han d'ésser observades per tot l'entorn de la **UNIVERSITAT AUTÒNOMA DE BARCELONA.**

**Confidencialitat**

1. Totes les dades de caràcter personal, han de tenir assegurat el correcte ús i l'estricte compliment ètic del tractament.

2. Només accediran a les dades, les persones que estiguin autoritzades, restringint el pas per al seu ús a totes les altres.

3. L'obligació del deure de secret afecta totes les persones que intervinguin en qualsevol fase del tractament de les dades de caràcter personal, fins i tot després d'haver finalitzat la relació amb el titular o el Responsable del Fitxer.

**Integritat**

1. Anomenada també qualitat de les dades, fa referència a què les dades siguin adequades, pertinents i no excessives en relació amb l'àmbit i finalitats legítimes per a les que s'hagin obtingut.

2. S'ha de garantir que totes les dades en possessió de la **UNIVERSITAT AUTÒNOMA DE BARCELONA**, siguin exactes i actuals, no es puguin deteriorar, estigui assegurada l'ètica en el tractament, tant intern com en possibles sortides, i que existeixi la garantia que no hi ha pèrdues d'informació.

3. S'està obligat a l'actualització permanent de les dades.

4. Les dades incorrectes o inexactes, seran cancel·lades o substituïdes per les correctes.

## Disponibilitat

1. S'haurà de garantir la disponibilitat de les dades de caràcter personal emmagatzemades als fitxers, mitjançant procediments que permetin la seva recuperació en cas de pèrdua o de desastre.

2. Les dades de caràcter personal s'emmagatzemaran de tal forma que permetin l'exercici dels drets d'accés, rectificació i cancel·lació per part de l'afectat.

## Intimitat

1. Queda totalment prohibit crear o mantenir fitxers amb la finalitat exclusiva d'emmagatzemar dades que revelin ideologia, religió, creences, origen racial i vida sexual.

2. Hi ha l'obligació en tots els casos, d'advertir als interessats del dret a no prestar el seu consentiment a donar dades especialment protegides o a cedir-les, excepte indicacions en contra.

## Ètica del Tractament

1. Queda prohibida la recollida de dades per mitjans fraudulents, deslleials o il·lícits.

2. Les dades no es podran usar per a finalitats diferents d'aquelles per a les quals van ésser recollides.

3. Tot el personal que hagi d'utilitzar dades de caràcter personal, haurà de comprometre's a guardar i observar les normes descrites en el present Document de Seguretat.

# DISTRIBUCIÓ DE COMPETÈNCIES I FUNCIONS

# 4. DISTRIBUCIÓ DE COMPETÈNCIES I FUNCIONS

## 4.1 Responsable del Fitxer

El Responsable del Fitxer de Dades de Caràcter Personal és la persona física o jurídica de naturalesa pública o privada designada i amb representació suficient, que decideix sobre la finalitat que se li va a donar a les dades contingudes als fitxers.

En *l'ANNEX 2.1 – PERSONES RESPONSABLES DE FITXER DE NIVELL ALT, l'ANNEX 2.2 – PERSONES RESPONSABLES DE FITXER DE NIVELL MITJÀ i l'ANNEX 2.3 – PERSONES RESPONSABLES DE FITXER DE NIVELL BAIX,* es relacionen els noms i cognoms dels Responsables de Fitxer.

**Funcions i Obligacions del Responsable de Fitxer**

En aquest apartat es relacionen les funcions dels Responsables de Fitxer amb Dades de Caràcter Personal:

1. Notificar per a la seva inscripció en el registre General de l'Agència de Protecció de Dades la creació, modificació i cancel·lació dels fitxers automatitzats que continguin dades de caràcter personal.

2. Vetllar pel compliment dels requisits establerts per la Llei Orgànica de Protecció de Dades i el Reglament de Mesures de Seguretat.

3. Comprovar el compliment i l'aplicació del Document de Seguretat.

4. Autoritzar la sortida de suports informàtics fora de les dependències de la **UNIVERSITAT AUTÒNOMA DE BARCELONA**, que continguin dades de caràcter personal extretes dels fitxers automatitzats dels que és responsable.

5. Nomenar un o diversos Responsables de Seguretat, encarregats de coordinar i controlar les mesures definides en el Document de Seguretat. En cap cas aquesta designació suposa una delegació de la responsabilitat que correspon al Responsable de Fitxer.

6. Adoptar les mesures correctores adequades, d'acord amb l'anàlisi dels informes d'auditoria realitzats pel Responsable de Seguretat.

7. Autoritzar per escrit els procediments de recuperació de dades.

## 4.2 Responsable de Seguretat

El Responsable de Seguretat de Dades és l'encarregat de vetllar pel compliment de tots els requisits establerts en la Llei Orgànica 15/1999, de 13 de desembre de Protecció de Dades de Caràcter Personal, en el Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, de les directrius i instruccions de l'Agència de Protecció de Dades i de qualsevol normativa vigent en matèria de seguretat de dades.

En *l'ANNEX 2.1 – PERSONES RESPONSABLES DE FITXER DE NIVELL ALT, l'ANNEX 2.2 – PERSONES RESPONSABLES DE FITXER DE NIVELL MITJÀ i l'ANNEX 2.3 – PERSONES RESPONSABLES DE FITXER DE NIVELL BAIX,* es relacionen els noms i cognoms dels Responsables de Seguretat.

El Responsable de Seguretat podrà comptar, en els casos que ho cregui convenient, amb la col·laboració i assessorament de les persones que consideri adequades.

**Funcions i Obligacions del Responsable de Seguretat**

Document de Seguretat

1. Redactar, establir i comprovar l'aplicació i el compliment del Document de Seguretat.

2. Actualitzar quan es requereixi, el Document de Seguretat dels fitxers automatitzats afectats per la LOPD.

3. Determinar l'àmbit d'aplicació del Document de Seguretat, definint i actualitzant els sistemes afectats pel present Document.

4. Coordinar, controlar i supervisar les activitats relacionades amb els fitxers automatitzats en matèria de seguretat

5. Coordinar i controlar les mesures definides en el Document de Seguretat.

6. Establir i comprovar l'aplicació de controls periòdics per verificar el compliment del què disposa el Document de Seguretat.

7. Elaborar un informe resum on s'especifiquen els controls efectuats per verificar que es compleix el Document de Seguretat, les anomalies i deficiències que en matèria de seguretat s'hagin detectat i una relació de les solucions i millores proposades.

Mesures de Seguretat

8. Recopilar i descriure les mesures, normes, procediments, regles i estàndards de seguretat adoptats per l'Organització.

9. Vetllar pel compliment de les normes de seguretat contingudes en el Document de Seguretat.

Funcions i Obligacions del Personal

10. Redactar les normes internes corresponents als usuaris.

11. Establir plans de formació, conscienciació i divulgació de les normes, obligacions i procediments de seguretat a la **UNIVERSITAT AUTÒNOMA DE BARCELONA**.

12. Vetllar pel compliment de les normes de seguretat, comunicant a RR.HH. les infraccions comeses, per a l'establiment de les corresponents sancions.

Registre d'Incidències

13. Supervisar i analitzar de forma periòdica les incidències succeïdes als centres, relacionades amb la seguretat dels fitxers automatitzats.

14. Establir i comprovar l'aplicació del procediment de notificació, tractament i registre d'incidències.

15. Elaborar un informe explicatiu d'aquelles incidències que afecten de manera greu als sistemes de seguretat de la **UNIVERSITAT AUTÒNOMA DE BARCELONA**.

16. Dictaminar mesures per donar resposta a les incidències greus succeïdes.

17. Fer el seguiment del registre d'incidències i ampliar els camps d'aquell per deixar constància dels procediments realitzats per a la recuperació de les

dades, indicant la persona que va executar el procés, les dades restaurades i, si és procedent, quines dades han sigut necessari gravar manualment en el procés de recuperació.

Control d'Accés Lògic - Identificació i Autenticació

18. Elaborar i mantenir actualitzada la llista d'usuaris que tinguin accés autoritzat al sistema informàtic, amb especificació del nivell d'accés que té cada usuari.

19. Establir i comprovar l'aplicació del procediment d'identificació i autenticació d'usuaris.

20. Establir i comprovar l'aplicació del procediment d'assignació, distribució i emmagatzematge de contrasenyes.

21. Comprovar el manteniment de la confidencialitat de les contrasenyes dels usuaris.

22. Establir i comprovar l'aplicació d'un procediment que garanteixi l'emmagatzematge de les contrasenyes vigents de forma inintel·ligible.

23. Establir i comprovar l'aplicació d'un sistema que limiti l'accés dels usuaris únicament a aquelles dades i recursos que es necessitin per al desenvolupament de llurs funcions.

24. Establir un mecanisme que permeti la identificació inequívoca i personalitzada de tot aquell usuari que intenti accedir al sistema i la verificació a la qual està autoritzat.

25. Establir i comprovar l'aplicació de mesures que impedeixin l'intent reiterat d'accedir de forma no autoritzada al sistema d'informació.

26. Establir els mecanismes necessaris per evitar que un usuari pugui accedir a dades o recursos amb drets distints dels autoritzats.

27. Concedir, alterar o anul·lar l'accés autoritzats a les dades i recursos, d'acord amb els criteris establerts pel Responsable de Fitxer.

Control d'Accés Físic

28. Establir i comprovar l'aplicació de mesures de control de l'accés físic als

locals on es trobin ubicats els sistemes d'informació amb dades de caràcter personal.

29. Comprovar que exclusivament el personal autoritzat, podrà accedir als locals on estiguin ubicats els sistemes informàtics.

Gestió de Suports

30. Establir i comprovar l'aplicació d'un sistema que permeti identificar, inventariar i emmagatzemar en lloc segur els suports informàtics que contenen dades de caràcter personal.

31. Establir i comprovar l'aplicació d'un registre d'entrada de suports informàtics que permeti, directa o indirectament, conèixer el tipus de suport, la data i hora, l'emissor, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable de la recepció que haurà d'estar degudament autoritzada.

32. Establir i comprovar l'aplicació d'un registre de sortida de suports informàtics que permeti, directa o indirectament, conèixer el tipus de suport, la data i hora, el destinatari, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable del lliurament que haurà d'estar degudament autoritzada.

33. Establir i comprovar l'aplicació de les mesures necessàries per impedir la recuperació posterior de la informació emmagatzemada en els suports informàtics que seran rebutjats o reutilitzats.

34. Establir i comprovar l'aplicació de les mesures necessàries per impedir la recuperació indeguda de la informació emmagatzemada en els suports informàtics que hagin de sortir fora dels locals en què es troben ubicats els fitxers.

35. Aquest punts només és aplicable als fitxers de Nivell Alt. Comprovar que la distribució dels suports que continguin dades de caràcter personal es realitzi xifrant les citades dades, o bé utilitzant qualsevol altre mecanisme que garanteixi que la citada informació no sigui intel·ligible ni manipulada durant el seu transport.

Còpies de Suport i Recuperació

36. Establir i comprovar l'aplicació del procediment de realització de còpies de suport i recuperació de dades.

37. Comprovar el compliment de la periodicitat establerta per a la realització de còpies de suport.

38. Autoritzar per escrit l'execució dels procediments de recuperació de dades.

39. Aquest punt només és aplicable als fitxers de Nivell Alt. Garantir que es conserva una còpia dels suports i els procediments de recuperació de dades en un lloc diferent del lloc a on es trobin els sistemes informàtics.

Proves amb Dades Reals

Aquest apartat només és aplicable als fitxers de Nivell Mitjà i Alt.

40. Comprovar que en la fase de proves dels sistemes d'informació, aquestes no s'efectuen amb dades personals reals o que aquestes compten amb les condicions de seguretat establertes.

Telecomunicacions

Aquest apartat només és aplicable als fitxers de Nivell Alt.

41. Comprovar que la transmissió de dades de caràcter personal a través de xarxes de telecomunicacions es realitza xifrant les citades dades o utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.

Registres d'accessos

Aquest apartat només és aplicable als fitxers de Nivell Alt.

42. Guardar de cada accés a les dades de nivell alt com a mínim:

- Identificació de l'usuari
- Data i hora de l'accés
- Fitxer accedit
- Concessió o denegació de l'accés.
- Identificar el registre accedit

43. Revisar periòdicament la informació de control registrada i elaborar un informe de les revisions realitzades i els problemes detectats, com a mínim un cop al mes.

44. Garantir que el registre d'accessos es guardarà com a mínim 2 anys.

Auditoria

Aquest apartat només és aplicable als fitxers de Nivell Alt.

45. Coordinar i controlar la realització d'una auditoria interna o externa sobre els sistemes d'informació i instal·lacions en què es porta a terme el tractament de les dades personals, que verifiqui el compliment del Reglament de Seguretat de la LOPD i dels procediments i instruccions vigents en matèria de seguretat de dades.

46. Analitzar els informes d'auditoria i elevar les conclusions al Responsable de Fitxer.

47. Adoptar les mesures correctores adequades, en funció de l'anàlisi dels informes d'auditoria realitzat pel Responsable de Seguretat.

48. Controlar que l'auditoria es realitzi, almenys, cada dos anys.

## 4.3 Encarregats del Tractament

Tindrà la condició d'encarregat del tractament, qualsevol prestador de serveis extern que, per prestar els serveis que se li encomanin, necessiti accedir o tractar dades de caràcter personal pertanyents als fitxers inclosos dins l'àmbit d'aplicació d'aquest Document.

Els encarregats dels tractaments tenen les obligacions que s'estableixen en la LOPD, i en els corresponents desplegaments reglamentaris. Tanmateix, les obligacions dels encarregats relatives a la protecció de dades de caràcter personal i a les mesures de seguretat aplicables, s'establiran expressament en cada cas, mitjançant la formalització d'un contracte, de conformitat amb l'establert a l'article 12 de la LOPD.

# FUNCIONS I OBLIGACIONS DEL PERSONAL

# 5. FUNCIONS I OBLIGACIONS DEL PERSONAL

## 5.1 Funcions i Obligacions del Personal

Amb l'objecte de donar degut compliment al que estableix l'art. 8.2.c del Reial Decret 994/1999 d'11 de juny, la **UNIVERSITAT AUTÒNOMA DE BARCELONA** obliga el seu personal al coneixement i compliment de les següents obligacions, les quals hauran d'ésser conegudes, acceptades i respectades per tot el personal.

Tindrà la consideració d'usuari qualsevol persona autoritzada a accedir a dades o recursos inclosos dins l'àmbit d'aplicació del Document de Seguretat de la Institució.

Dins del col·lectiu d'usuaris cal diferenciar un cas especial: els usuaris administradors. Com a conseqüència de la seva activitat professional poden tenir un accés a la informació, sense les restriccions que tenen la resta d'usuaris. Aquests privilegis són necessaris per a la correcta gestió dels sistemes d'informació on resideixen els fitxers amb dades de caràcter personal.

Donada aquesta circumstància caldrà que aquests usuaris estiguin explícitament identificats, així com el rol a desenvolupar (administradors de bases de dades, tècnics de sistemes, responsables d'aplicacions informàtiques, operadors, manteniment d'equips informàtics, etc.).

En cas que existeixin usuaris que no formin part del personal al servei de la **UNIVERSITAT AUTÒNOMA DE BARCELONA,** les seves obligacions i responsabilitats hauran d'estar clarament especificades mitjançant la formalització d'un contracte, pacte, acord o qualsevol altre acte equivalent que permeti acreditar l'establiment de les obligacions i responsabilitats corresponents, així com el compromís d'acomplir-les.

### Obligacions de tot el personal de la UNIVERSITAT AUTÒNOMA DE BARCELONA

### Confidencialitat de la Informació:

1. Els usuaris dels sistemes d'informació i dels fitxers amb dades de caràcter personal hauran de guardar, per temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni a través de terceres persones o

empreses, les dades, documents, metodologies, claus, anàlisi, programes i la resta d'informació a què tinguin accés durant la seva relació laboral amb la **UNIVERSITAT AUTÒNOMA DE BARCELONA** tant en suport material com electrònic. Aquesta obligació continuarà vigent després de l'extinció de la seva relació amb el titular del fitxer o el seu responsable.

2. Queda prohibit trametre informació confidencial de l'Organització a l'exterior, mitjançant suports materials, o a través de qualsevol mitjà de comunicació, incloent la simple visualització o accés, excepte autorització expressa del Responsable de Fitxer.

3. Cap col·laborador haurà de posseir, per a usos no propis de la seva responsabilitat, cap material o informació propietat de l'Organització, tant ara com en el futur.

4. En el cas que, per motius directament relacionats amb el lloc de treball, l'empleat entri en possessió d'informació confidencial sota qualsevol tipus de suport, haurà d'entendre's que la citada possessió és estrictament temporal, amb obligació de secret i sense que això li atorgui cap dret de possessió, o titularitat o còpia, cobri la referida informació.

5. Així mateix, el treballador haurà de tornar els citats materials a l'Organització o destruir-los, immediatament després de la finalització de les tasques que han originat l'ús temporal dels mateixos, i en qualsevol cas, a la finalització de la relació laboral.

## Codis d'identificació i Claus d'Accés:

1. Queda prohibit comunicar a una altra persona l'identificador d'usuari i la clau d'accés. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i d'accés, haurà de posar-ho en coneixement del responsable del sistema, a fi que li assigni una nova clau. Davant d'una baixa o absència temporal de l'usuari, el responsable del departament podrà sol·licitar al responsable del sistema la cessió de clau o dades a la persona per ell designada, havent de quedar registrada per escrit la citada autorització.

2. L'usuari està obligat a utilitzar la xarxa corporativa i la intranet de l'organització i les seves dades sense incórrer en activitats que puguin ésser considerades il·lícites o il·legals, que infringeixin els drets de l'organització o de tercers, o que puguin atemptar contra la moral o les normes d'etiqueta de les xarxes telemàtiques.

3. Estan expressament prohibides les següents activitats:

    - Compartir o facilitar l'identificador d'usuari i la clau d'accés facilitats per l'organització amb una altra persona física o jurídica, inclòs el personal de la pròpia organització. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable dels actes realitzats per la persona física o jurídica que utilitzi de forma no autoritzada l'identificador de l'usuari.

    - Intentar distorsionar o falsejar els registres d'activitat històrics (LOG) del Sistema.

    - Intentar desxifrar les claus, sistemes o algoritmes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de l'organització.

    - Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris (Aquesta activitat pot constituir un delicte d'intercepció de les telecomunicacions previst a l'article 197 del Codi Penal).

    - Utilitzar el sistema per intentar accedir a àrees restringides dels sistemes informàtics de l'Organització o de tercers.

    - Intentar augmentar el nivell de privilegis d'un usuari en el sistema.

**Utilització dels Recursos Informàtics:**

Els usuaris amb accés als sistemes informàtics i de xarxa hauran d'esforçar-se en fer servir i promoure un ús eficient d'aquests recursos, a fi d'evitar tràfic innecessari i interferències en el treball d'altres usuaris.

Per això, estaran expressament prohibides les següents activitats:

- Destruir, alterar, inutilitzar o de qualsevol altra forma danyar les dades, programes o documents electrònics de l'organització o de tercers (poden constituir un delicte de danys, previst a l'article 264.2 del Codi Penal).

- Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics de l'organització, així com realitzar accions que danyin, interrompin o generin errors en els sistemes citats.

- Trametre missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitàries sense el consentiment del destinatari (Spam).

- Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin o siguin susceptibles de causar qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o de tercers. L'usuari tindrà l'obligació, seguint les directrius marcades pels serveis informàtics, d'utilitzar els programes antivírics i les actualitzacions per prevenir l'entrada en el sistema de qualsevol element destinat a destruir o corrompre les dades informàtiques.

- Introduir, descarregar d'internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per l'organització, o qualsevol altre tipus d'obra o material els drets de propietat intel·lectual o industrial que pertanyin a tercers, quan no es disposi d'autorització per a això.

- Instal·lar còpies il·legals de qualsevol programa, inclosos els estandarditzats i els de caràcter gratuït.

- Esborrar qualsevol dels programes instal·lats legalment.

- Utilitzar els recursos telemàtics de l'organització, inclosa la xarxa Internet, per a activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.

- Introduir continguts obscens, immorals o ofensius i, en general, mancats d'utilitat per als objectius de l'organització, a la xarxa corporativa de l'Organització.

- Trametre o retransmetre missatges en cadena o de tipus piramidal.

**<u>Utilització del Correu Electrònic:</u>**

1. El sistema informàtic, la xarxa corporativa i els terminals utilitzats per cada usuari són propietat de l'organització.

2. Es considerarà correu electrònic tant l'intern, entre terminals de la xarxa corporativa, com l'extern, dirigit o provenint d'altres xarxes públiques o privades i especialment internet. Cap missatge de correu electrònic serà

considerat com a privat.

3. El servei de correu electrònic ha d'ésser usat únicament per a la comunicació d'aspectes relacionats amb el negoci i/o el compliment de les obligacions laborals.

4. L'organització vetllarà pel correcte ús del correu electrònic dels usuaris de la xarxa corporativa i els arxius de registres històrics d'activitat (LOG) del servidor, a fi de comprovar el compliment d'aquestes normes i prevenir activitats que puguin afectar a l'organització com a responsable civil subsidiària del mal ús d'aquest recurs.

5. Qualsevol fitxer introduït a la xarxa corporativa o al terminal de l'usuari a través de missatges de correu electrònic que provinguin de xarxes externes, haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

## Utilització de l'Accés a Internet:

1. L'ús del sistema informàtic de l'organització per accedir a xarxes públiques com internet, es limitarà als temes directament relacionats amb l'activitat de l'organització i les funcions del lloc de treball de l'usuari.

2. L'accés a debats en temps real (Xat / IRC) és especialment perillós, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, per la qual cosa el seu ús queda estrictament prohibit.

3. L'accés a pàgines Web, grups de notícies (Newsgroups) i altres fonts d'informació com FTP, telnet, etc. es limita a aquells que continguin informació relacionada amb l'activitat de l'organització o amb les funcions del lloc de treball de l'usuari.

4. L'organització es reserva el dret de monitoritzar i comprovar, de forma aleatòria i sense previ avís, qualsevol sessió d'accés a internet iniciada per un usuari de la xarxa corporativa.

5. Qualsevol fitxer introduït a la xarxa corporativa o al terminal de l'usuari des d'Internet, haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

## Propietat Intel·lectual i Industrial:

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

**Gestió d'Incidències:**

S'entén per incidència qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades.

1. És obligació de tot el personal de l'organització comunicar al responsable del sistema qualsevol incidència que es produeixi en els sistemes d'informació a què tinguin accés.

2. La citada comunicació haurà de realitzar-se immediatament i, en qualsevol cas, en un termini de temps no superior a una hora (1) des del moment en què es conegui la citada incidència.

**Protecció de dades:**

Es consideraran actes prohibits:

1. Crear fitxers de dades personals sense l'autorització del Responsable de Fitxer.

2. Utilitzar les dades personals per a finalitats incompatibles amb aquelles per les que s'hagin recaptat o per a finalitats diferents de les comunicades a l'Agència de Protecció de Dades.

3. Creuar informació relativa a dades de diferents fitxers o serveis a fi d'establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sense l'autorització expressa del Responsable de Fitxer.

4. Qualsevol altra activitat expressament prohibida en aquest document o en les normes sobre protecció de dades i Instruccions de l'Agència de Protecció de Dades.

## 5.2 Comunicació

Correspon a la institució l'adopció de les mesures que permetin al personal conèixer les normes de seguretat relacionades amb el desenvolupament de les seves funcions, així com de les conseqüències del seu incompliment.

Les normes contingudes en el paràgraf anterior s'inclouran en el Document "*Normes de Seguretat dels Sistemes d'Informació*" i es donaran a conèixer formalment i de forma individualitzada entre tot el personal que presti servei actualment a la institució. A tots els efectes signaran la recepció de les normes i el seu coneixement.

En aquest mateix document, s'integraran de forma explicativa les conseqüències i responsabilitats que l'incompliment de les esmentades funcions li pot suposar a tots els nivells, incloent el laboral.

Les persones que entren a prestar servei a la institució amb caràcter temporal o indefinit, procediran a rebre formalment i de forma individualitzada les normes de seguretat dels sistemes d'informació, en el moment de firmar el contracte de treball, contracte administratiu o acta de presa de possessió.

Aquesta mateixa política, on s'inclouen totes les obligacions genèriques que afecten als empleats en quant a la seguretat dels tractaments de dades i l'ús dels sistemes d'informació, pot penjar-se a la intranet o a qualsevol sistema d'informació massiu.

Sempre que sigui necessari, i en qualsevol cas, amb una periodicitat mínima anual, es remetrà una circular informativa fent referència a les possibles modificacions produïdes en les normes de seguretat dels sistemes d'informació.

## 5.3 Responsabilitat

L'incompliment de les obligacions per part del personal serà sancionat disciplinadament, prèvia instrucció del preceptiu expedient.

D'igual manera, sense perjudici de la responsabilitat disciplinària corresponent que pugui incórrer el personal, s'exigirà d'ofici la corresponent responsabilitat pels danys i perjudicis ocasionats als particulars, sempre que hagi existit dol o culpa greu.

La responsabilitat penal i la responsabilitat civil derivada del delicte en què hagi incorregut el personal, s'exigirà de conformitat amb la legislació corresponent.

# GESTIÓ DE FITXERS

# 6. GESTIÓ DE FITXERS

## 6.1 Sistemes d'Informació

La Llei entén com a Sistema d'informació, el conjunt de fitxers automatitzats, programes, suports i equips emprats per a l'emmagatzematge i tractament de dades de caràcter personal.

Els Sistemes d'Informació que donen suport a les àrees descrites, són els especificats en *l'ANNEX 4 – DESCRIPCIÓ GENERAL DELS SISTEMES D'INFORMACIÓ*, que contenen aplicacions i fitxers amb recursos protegits a la **UNIVERSITAT AUTÒNOMA DE BARCELONA.**

Qualsevol modificació en aquestes aplicacions, haurà d'ésser oportunament informada al Responsable de Seguretat per si afectés al present Document de Seguretat i a les Dades de Caràcter Personal.

## 6.2 Fitxers i Estructures

Es considera Fitxer automatitzat a tot conjunt organitzat de caràcter personal que sigui objecte d'un tractament automatitzat, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés.

En *l'ANNEX 1.1 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL ALT, l'ANNEX 1.2 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL MITJÀ i l'ANNEX 1.3 – INVENTARI DE FITXERS AMB DADES DE CARÀCTER PERSONAL DE NIVELL BAIX,* es relacionen tots el fitxers automatitzats que han sigut identificats per cada un dels Responsables de la **UNIVERSITAT AUTÒNOMA DE BARCELONA,** com a subjectes al reglament de mesures de seguretat dels fitxers automatitzats que contenen dades de caràcter personal.

Aquest Annex conté a més les estructures dels fitxers que han sigut inventariats, ressaltant aquells camps que es consideren afectats per la llei.

## 6.3 Fitxers Temporals

És norma comuna de tots, la de crear fitxers d'ús personal extrets dels que es troben en els servidors centrals, o bé dels impresos, llistats, etc., per a la seva utilització en algun assumpte determinat i amb una duració temporal.

Per tant, i respecte als fitxers creats per a l'ús Personal o com a fitxers temporals s'han de seguir les següents normes:

1. Es permet la creació de fitxers de treball temporals o d'ús personal, amb dades extretes dels fitxers centrals o d'impresos, llistats, etc.

2. Els fitxers temporals han de mantenir els criteris exigits en la normativa de seguretat quant a confidencialitat (limitació de l'accés a la informació), integritat i disponibilitat.

3. S'ha de mantenir la intimitat (deure de secret) i la privacitat de les dades de caràcter personal recollides en els fitxers citats.

4. Les dades de caràcter personal incloses en aquests fitxers no podran ésser utilitzades per a finalitats diferents d'aquelles per a les que van ésser inicialment recollides.

5. No s'han de crear fitxers amb la finalitat exclusiva d'emmagatzemar dades de caràcter Personal que revelen la ideologia, afiliació sindical, religió, creences, origen racial o ètnic, o vida sexual.

6. Les dades de caràcter personal recollides als fitxers personals o temporals, seran adequades, pertinents i no excessives en relació amb la finalitat per a la que s'hagi creat el fitxer.

7. Les dades de caràcter personal recollides hauran d'ésser actualitzades de forma permanent, sent les incorrectes cancel·lades o substituïdes per les correctes.

8. Els fitxers no podran ésser conservats una vegada deixin d'ésser útils per a la funció prevista.

La normativa sobre fitxers temporals es transmetrà a tots els usuaris dels sistemes d'informació de la **UNIVERSITAT AUTÒNOMA DE BARCELONA**, mitjançant el document "*Normes de Seguretat dels Sistemes d'Informació*".

### 6.4 Proves amb Dades Reals

Per a les Proves amb dades reals, quan s'obtinguin dades de fitxers que tinguin la qualificació de mitja o alta segons la LODP es procedirà a la seva desnaturalització, mitjançant:

1. Canvi de les dades identificadores, per altres irrellevants.

2. Eliminació de les dades identificades i els seus codis, de forma que no es corresponguin de cap manera les dades identificadores i els seus propietaris.

No serà necessària la desnaturalització per a les proves que incloguin les mesures de seguretat dels fitxers reals.

# GESTIÓ D'INCIDÈNCIES

# 7. GESTIÓ D'INCIDÈNCIES

## 7.1 Normes Generals

Serà necessari notificar i gestionar les incidències amb un registre en el que consti el tipus d'incidència, el moment en què es produeix, la persona que realitza la notificació, a qui ho comunica i els efectes derivats d'aquesta. Aquest registre serà habilitat pel responsable de seguretat, i estarà a disposició de tots els usuaris dels fitxers, amb la finalitat de que es registre tota incidència que pugui suposar un perill per a la seguretat del mateix.

En el registre d'incidències, hauran de consignar-se a més, els procediments realitzats de recuperació de les dades restaurades i si és procedent, quines dades ha sigut necessari gravar manualment en el procés de recuperació.

Qualsevol usuari que tingui coneixement d'una incidència haurà de posar-la en coneixement del responsable de seguretat per tal de ser enregistrada.

Serà necessària l'autorització per escrit del Responsable de Fitxer per a l'execució dels procediments de recuperació de les dades.

## 7.2 Procediment

Amb l'objecte de donar el degut compliment adequat al que estableix l'Art. 8.2.e del Real Decret 994/1999 d'11 de juny, la **UNIVERSITAT AUTÒNOMA DE BARCELONA** disposa d'un procediment de notificació, gestió i resposta de les incidències, entenent per incidència qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades.

L'objecte d'aquest procediment és establir un mètode de registre i gestió de les incidències que puguin succeir durant l'explotació dels Sistemes d'Informació a la **UNIVERSITAT AUTÒNOMA DE BARCELONA** i que tractin dades de caràcter personal.

El procediment es troba descrit en *l'ANNEX 7 – PROCEDIMENT DE NOTIFICACIÓ I GESTIÓ D'INCIDÈNCIES* del present Document de Seguretat.

# IDENTIFICACIÓ I AUTENTICACIÓ D'USUARIS

# 8. IDENTIFICACIÓ I AUTENTICACIÓ D'USUARIS

## 8.1 Normes Generals

El Responsable de Fitxer s'encarregarà que existeixi una relació actualitzada d'usuaris que tinguin accés al sistema d'informació i d'establir procediments d'identificació i autenticació per l'accés.

Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes existirà un procediment d'assignació, distribució i emmagatzematge que garanteixi la seva confidencialitat i integritat.

Les contrasenyes es canviaran amb la periodicitat que es determini en aquest Document de Seguretat i mentre estiguin vigents s'emmagatzemaran de forma inintel·ligible.

Igualment s'aplicaran aquestes garanties a futurs mecanismes d'autenticació que puguin implementar-se (certificats digitals, identificacions biomètriques, etc).

El Responsable de Fitxer establirà un mecanisme que permeti la identificació de forma inequívoca i personalitzada de tot aquell usuari que intenta accedir al sistema d'informació i la verificació a la qual està autoritzat.

Es limitarà la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

## 8.2 Procediment

A l'*ANNEX 8* – es descriu el *PROCEDIMENT D'IDENTIFICACIÓ I AUTENTICACIÓ D'USUARIS*.

# GESTIÓ D'ACCÉS LÒGIC

# 9. GESTIÓ D'ACCÉS LÒGIC

## 9.1 Normes Generals

Els usuaris tindran accés autoritzat únicament a aquelles dades i recursos que es necessitin per al desenvolupament de les seves funcions.

El Responsable de Fitxer establirà mecanismes per evitar que un usuari pugui accedir a dades o recursos amb drets distints dels autoritzats.

La relació d'usuaris amb accés autoritzat al sistema d'informació, contindrà l'accés autoritzat per a cada un d'ells.

Exclusivament el personal autoritzat en el Document de seguretat podrà concedir alterar o anul·lar l'accés autoritzat sobre les dades i recursos, conforme als criteris establerts pel Responsable de Fitxer.

## 9.2 Procediments

El Responsable de Seguretat, serà el responsable, de concedir, alterar o anul·lar l'accés autoritzat sobre les dades i recursos afectats i indicats en els apartats corresponents d'aquest Document de Seguretat.

D'igual manera serà el responsable de fer complir els controls d'accés lògic i informar els usuaris dels deures i responsabilitats de llur incompliment, mitjançant accions de formació i sistemes de comunicació continuat.

A l'*ANNEX 8 - PROCEDIMENT D'IDENTIFICACIÓ I AUTENTICACIÓ D'USUARIS* es descriuen els procediments de control d'accés lògic.

# CÒPIES DE SEGURETAT I RECUPERACIÓ DE DADES

# 10.CÒPIES DE SEGURETAT I RECUPERACIÓ DE DADES

## 10.1 Normes Generals

El Responsable de Fitxer s'encarregarà de verificar la definició i correcta aplicació dels procediments de realització de còpies de suport i de recuperació de les dades.

Els procediments establerts per a la realització de còpies de suport i per a la recuperació de les dades, hauran de garantir la seva reconstrucció en l'estat en què es trobaven al temps de produir-se la pèrdua o destrucció.

Hauran de realitzar-se còpies de suport, almenys setmanalment, llevat que en el període no s'hagués produït cap actualització de les dades.

Per als fitxers amb dades personal de Nivell Alt, i no per als de Nivells Mitjà o Baix, haurà de conservar-se una còpia de seguretat i dels procediments de recuperació de les dades, en un lloc diferent d'aquell en què es troben els equips informàtics que els tractin complint en tot cas, les mesures de seguretat exigides en el Reglament.

Serà necessària l'autorització del Responsable de Fitxer per a l'execució de procediments de recuperació de dades, i deurà quedar constància la registre d'incidències de les manipulacions que hagin estat necessàries per a la recuperació, identificant la persona que ha realitzat el procés, les dades restaurades i les que s'hagin gravat manualment en el procés de recuperació.

## 10.2 Procediment

Amb l'objecte de donar degut compliment al que estableix l'Art. 8.2.F del Real Decret 994/1999 d'11 de juny, la **UNIVERSITAT AUTÒNOMA DE BARCELONA** disposa d'un procediment de realització de còpies de suport i recuperació de dades que garanteix la seva reconstrucció en l'estat en què es trobessin al temps de produir-se la pèrdua o destrucció.

En l'*ANNEX 9 - PROCEDIMENTS DE CÒPIES DE SEGURETAT I RECUPERACIÓ DE DADES* es descriuen aquests procediments.

# GESTIÓ DE SUPORTS

# 11. GESTIÓ DE SUPORTS

## 11.1 Normes Generals

Els suports informàtics que continguin dades de caràcter personal pertanyents a la **UNIVERSITAT AUTÒNOMA DE BARCELONA** incloses dins l'àmbit d'aplicació d'aquest document, hauran de permetre identificar el tipus d'informació que contenen. Així mateix, estaran emmagatzemades i convenientment inventariades en un lloc específic destinat a tal efecte.

La sortida de suports informàtics fora de les dependències del seu centre de tractament únicament podrà ser autoritzada pel Responsable de Fitxer. A aquests efectes, el Responsable de Seguretat s'encarregarà de la gestió, arxiu i custòdia d'aquestes autoritzacions.

Quan es procedeixi a desprendre's o a reutilitzar un suport automàtic amb dades de caràcter personal, prèviament a la seva baixa o modificació en l'inventari, s'impedirà qualsevol recuperació posterior de les dades arxivades en aquell mitjançant l'aplicació d'un procés de desgravació completa de la informació. En cas que aquest procés no sigui possible, el suport no serà reutilitzat i es procedirà a la seva inutilització o destrucció física.

Els fitxers de dades de caràcter personal inclosos dins l'àmbit d'actuació del present document, hauran de disposar d'un registre d'entrades i sortides de suports informàtics que els tractin en els respectius centres de tractament.

Si, com a conseqüència d'operacions de manteniment d'equipaments informàtics, fos necessària la sortida de suports fora de les dependències del seu centre de tractament, s'adoptaran les mesures adients per impedir qualsevol recuperació indeguda de la informació que en ells s'arxiva.

## 11.2 Procediments

En *l'ANNEX 10 – PROCEDIMENTS PER A LA GESTIÓ DE SUPORTS* es descriuen els procediments d'identificació, inventari, custòdia, registre i destrucció de suports informàtics amb dades de caràcter personal.

# CONTROL D'ACCÉS FÍSIC

# 12. CONTROL D'ACCÉS FÍSIC

Aquest capítol només és aplicable als fitxers amb dades de caràcter personal de Nivell Mitjà i Alt.

## 12.1 Normes Generals

Exclusivament el personal autoritzat en el Document de Seguretat podrà tenir accés als locals, on es troben ubicats els sistemes d'informació amb dades de caràcter personal.

## 12.2 Procediments

En *l'ANNEX 11 – PROCEDIMENT PER A L'ACCÉS FÍSIC* es descriuen els procediments per limitar l'accés a les persones autoritzades.

# REGISTRE D'ACCESSOS

# 13. REGISTRE D'ACCESSOS

Aquest capítol només és aplicable als fitxers amb dades de caràcter personal de Nivell Alt.

## 13.1 Normes Generals

Per als fitxers amb dades de caràcter personal de nivell alt, de cada accés es guardaran, com a mínim, la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer accedit, el tipus d'accés i si ha sigut autoritzat o denegat.

En el cas que l'accés hagi estat autoritzat, serà necessari guardar la informació que permeti identificar el registre accedit.

Els mecanismes que permeten el registre de dades detallades en els punts anteriors, estaran sota el control directe del Responsable de Seguretat competent sense que s'hagi de permetre, en cap cas, la desactivació d'aquests.

El període mínim de conservació de les dades serà de dos anys.

El Responsable de Seguretat competent s'encarregarà de revisar periòdicament la informació de control registrada i elaborarà un informe de les revisions realitzades i els problemes detectats almenys una vegada al mes.

## 13.2 Procediments

A *l'ANNEX 13 – PROCEDIMENT DE REGISTRE D'ACCESSOS ALS FITXERS DE NIVELL ALT*, es presenta el flux a seguir per a realitzar i monitoritzar aquest tipus de registres.

# TELECOMUNICACIONS

# 14.TELECOMUNICACIONS

Aquest capítol només és aplicable als fitxers amb dades de caràcter personal de Nivell Alt.

## 14.1 Normes Generals

Aquest apartat descriu la normativa a aplicar per implantar una solució de seguretat en comunicacions sobre els sistemes d'informació que manegen dades de caràcter personal de Nivell Alt a la **UNIVERSITAT AUTÒNOMA DE BARCELONA**.

Les xarxes locals dels centres i dependències de la **UNIVERSITAT AUTÒNOMA DE BARCELONA** i la xarxa que intercomunica a tots els centres entre si, mantindran un sistema de seguretat en les comunicacions per a les dades de caràcter personal.

El sistema de seguretat contemplarà almenys els serveis d'autenticació, confidencialitat i integritat de dades.

Servei d'Autenticació:

Mitjançant aquest servei s'assegura la identificació dels extrems en les sessions de diàleg entre un lloc PC i el servidor d'aplicacions a fi d'evitar la pèrdua d'informació per tramesa a destins incorrectes, mantenint la confidencialitat i assegurant la suplantació de tercers.

Servei de Confidencialitat:

Aquest servei assegura la confidencialitat de la informació circulant a través de les línies (protecció contra atacs passius).

Aquest servei evita la legitimitat a tercers de la informació circulant, mitjançant el xifrat (encriptació) de les dades.

Servei d'Integritat.

La implantació d'aquest servei assegura la integritat de la informació circulant a través de les distintes línies de la xarxa de comunicacions (protecció contra atacs actius).

Amb aquest servei s'evita la inserció, esborrat o modificació de la informació

original.

Es podran transmetre dades de caràcter personal de nivell alt a entitats externes a la **UNIVERSITAT AUTÒNOMA DE BARCELONA** a través de xarxes de telecomunicacions sempre amb l'autorització del Responsable de Fitxer de què provenen les dades i en tot cas xifrant (encriptant) les citades dades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulable per tercers.

## 14.2 Procediments

En *l'ANNEX 14 – TRANSMISSIÓ DE DADES DE NIVELL ALT, es presenta el procediment per a la transmissió d'aquest tipus de dades.*

# CONTROLS INTERNS I AUDITORIES

# 15.CONTROLS INTERNS I AUDITORIES

## 15.1 Normes Generals

Per verificar l'acompliment del què disposa el Document de Seguretat es realitzaran controls interns. Aquests controls s'iniciaran d'ofici, per part del Responsable de Seguretat o pel Responsable de Fitxer, i haurien de realitzar-se amb una freqüència mínima d'una vegada a l'any.

Igualment, la realització de l'auditoria periòdica permet verificar si els controls establerts a través de les mesures de seguretat són efectius i si és possible garantir la integritat, confidencialitat i disponibilitat de les dades de caràcter personal.

Igualment, permet garantir que l'empresa compleix amb allò que demana el Reglament de Mesures de Seguretat de cara a una possible inspecció de l'Agència de Protecció de Dades.

## 15.2 Procediments

Aquest apartat defineix la normativa a aplicar per a la realització d'auditories de seguretat de dades a la **UNIVERSITAT AUTÒNOMA DE BARCELONA**, a fi de confirmar que les pràctiques i mesures de seguretat aplicades, són les adequades i que segueixen les normes i procediments indicats en el Document de Seguretat.

La **UNIVERSITAT AUTÒNOMA DE BARCELONA** realitzarà auditories de seguretat LOPD amb una periodicitat mínima biennal. Les auditories es realitzaran per personal propi o bé es delegarà la seva realització a empreses consultores externes.

Les auditories han de contemplar almenys els següents punts:

- Adequació de la normativa, procediments i controls contemplats en el Document de Seguretat, segons el que disposa el Reglament de Seguretat de la LOPD i a les disposicions legals que en matèria de dades de caràcter personal puguin establir en el futur les autoritats competents.

- Verificar, per a les instal·lacions i sistemes d'informació que manegen dades de caràcter personal, el correcte compliment de les mesures, procediments i normatives que en matèria de seguretat s'estableixin en el present Document.

- Identificació de les deficiències que en matèria de seguretat LOPD es troben a les instal·lacions, sistemes d'informació, normatives, procediments i pràctiques a la **UNIVERSITAT AUTÒNOMA DE BARCELONA**.

- Establiment de mesures i recomanacions per resoldre les deficiències trobades.

- Inclusió de totes aquelles dades, fets i observacions en què es basen els dictàmens, recomanacions i propostes emeses.

Els controls interns i d'auditoria actuaran en les següents àrees:

- Control de l'aplicació del Document de Seguretat.

- Control del sistema d'identificació i autenticació.

- Control del sistema de control d'accés.

- Control del compliment de les normes de confidencialitat i secret.

- Control del compliment de les normes internes i les funcions del personal.

- Control dels procediments de gestió de suports.

- Control antivirus.

El contingut de les auditories (tant si són internes com externes) serà analitzat pel Responsable de Seguretat, el qual elaborarà un document de conclusions per al Responsable de Fitxer.

Les auditories realitzades, conjuntament amb els informes de conclusions, es dipositaran i arxivaran, mantenint tant les auditories com els informes a disposició de l'Agència de Protecció de Dades.

# GESTIÓ DEL DOCUMENT DE SEGURETAT

# 16.GESTIÓ DEL DOCUMENT DE SEGURETAT

El Document estarà en tot moment actualitzat i serà revisat sempre que es produeixin canvis rellevants en els sistemes d'informació o en l'organització de la **UNIVERSITAT AUTÒNOMA DE BARCELONA.**

El contingut del Document haurà d'adequar-se, en tot moment, a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

## 16.1 Actualització del Document de Seguretat

L'objecte d'aquest procediment és establir un sistema d'operació en l'actualització i difusió del Document de Seguretat d'adequació a la LOPD a la **UNIVERSITAT AUTÒNOMA DE BARCELONA**.

El control i verificació de la correcta aplicació d'aquest procediment recau en el Responsable de Seguretat.

El Document de Seguretat d'adequació a la LOPD estableix l'organització, normatives i procediments de seguretat d'obligat compliment per al personal amb accés als sistemes d'informació i dades automatitzades de caràcter personal.

El citat Document ha de mantenir-se en tot moment actualitzat i ha d'ésser revisat obligatòriament sempre que es produeixin canvis rellevants en l'organització de seguretat, en els sistemes d'informació o quan sigui necessari adequar-se a les disposicions vigents que en matèria de seguretat de dades de caràcter personal, estableixin les autoritats competents.

Observacions:

Sempre que una persona cessi en les funcions que li permetin disposar del Document de Seguretat d'adequació a la LOPD haurà de tornar al Responsable de Seguretat els documents que romanguin en el seu poder.

## 16.2 Descripció del Procediment

En les pàgines següents es recull la descripció del procediment.

**Modificació en l'estructura dels sistemes d'informació**

Si es produeix una modificació en l'estructura dels sistemes d'informació que contenen dades de caràcter personal, el responsable tècnic del sistema afectat elabora una "Proposta concreta de canvi" i la remet al Responsable de Seguretat en mà o per correu electrònic.

**Responsables de Fitxer**

Si algun Responsable de Fitxer considera necessari modificar l'estructura de dades dels fitxers automatitzats dels que n'és responsable, elabora una "Proposta concreta de canvi" i la remet al Responsable de Seguretat en mà o per correu electrònic.

Estudi d'actualització del ***Document de Seguretat***

**Responsable de Seguretat**

Rebuda la "Proposta concreta de canvi", el Responsable de Seguretat estudia les modificacions a incorporar al Document de Seguretat.

Així mateix, el Responsable de Seguretat també estudia les modificacions a incorporar en el Document de Seguretat, si es produeix una incidència greu en un sistema d'informació que obligui a la seva modificació, o canvia la legislació vigent que afecti a les normes o procediments.

Elaboració de l'esborrany del ***Document de Seguretat***

Si ho considera oportú i a la vista de la modificació a introduir en el Document de Seguretat, el Responsable de Seguretat elabora un esborrany del nou Document de Seguretat i l'eleva al Responsable de Fitxer per al seu estudi i aprovació.

Estudi i aprovació de l'esborrany del ***Document de Seguretat***

El Responsable de Fitxer estudia i aprova, si ho considera pertinent, el nou Document de Seguretat, i autoritza la seva difusió a les diverses unitats de negoci

Emissió i difusió del ***Document de Seguretat***

Aprovada la nova versió del Document i la seva difusió, el Responsable de Seguretat elabora un "Resum explicatiu dels canvis efectuats" i l'adjunta al Document de Seguretat.

El Responsable de Seguretat s'encarrega de l'emissió i difusió de les diferents revisions del Document a les persones autoritzades a posseir una còpia d'aquest.

Actualització del registre de versions del ***Document de Seguretat***

Amb cada revisió del Document, el Responsable de Seguretat actualitzarà el "Registre de versions del Document de Seguretat".