RESOLUCIÓ de 12 de març de 2013, de la Direcció General de Centres i Personal Docent, de la Conselleria d'Educació, Cultura i Esport, per la qual es dicten instruccions en matèria de seguretat dels sistemes de videovigilància dels centres educatius públics de titularitat de la Generalitat.

La Llei Orgànica 2/2006, de 3 de maig, d'Educació, determina que els responsables de l'educació han de proporcionar als centres els recursos i els mitjans que necessiten per a desenrotllar la seua activitat i aconseguir este objectiu, mentres que estos han d'utilitzar-los amb rigor i eficiència per a complir la seua comesa de la millor manera possible. És necessari, per tant, que la normativa combine ambdós aspectes, i establisca les normes comunes que tots han de respectar, així com l'espai d'autonomia que s'ha de concedir als centres docents.

D'esta manera, vista la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (d'ara en avant LOPD), així com la Instrucció 1/2006, de 8 de novembre, sobre el tractament de dades personals amb fins de vigilància a través de sistemes de càmeres o videocàmeres, de l'Agència Espanyola de protecció de dades (d'ara en avant AEPD), la direcció general competent en matèria de centres docents ha de proporcionar un extracte d'obligacions de seguretat dels sistemes de videovigilància aplicables a tots aquells centres educatius públics de titularitat de la Generalitat. Convé, per tant, dictar instruccions respecte a les mesures de centres educatius públics que instal·len sistemes de videovigilància i on a més existisca un tractament de les imatges (gravació, captació, transmissió, conservació, o emmagatzematge d'imatges, incloent-n'hi la reproducció o emissió en temps real o un tractament que resulte de les dades personals relacionats amb aquelles).

Per tot això, i en virtut de les competències establides en el Decret 190/2012, de 21 de desembre, del Consell, pel qual s'aprova el Reglament Orgànic i Funcional de la Conselleria d'Educació, Cultura i Esport, resolc:

Apartat únic

1. Aprovar les instruccions incloses en l'annex I, a les quals hauran d'ajustar-se els centres educatius públics de titularitat de la Generalitat que tinguen instal·lat prèviament a la publicació d'esta instrucció un sistema de videovigilància en les seues instal·lacions o hagen d'instal·lar-lo.
2. Establir els models d'informació que figuren en l'annex II.
3. Aprovar les mesures de seguretat de nivell bàsic que s'arrepleguen en els annexos III i IV.

València, 12 de març de 2013
El director general de Centres i Personal Docent

Santiago Martí Alepuz

ANNEX I

Instruccions en matèria de seguretat dels sistemes de videovigilància dels centres educatius públics de titularitat de la Generalitat

1. Normes generals d'ús i instal·lació dels sistemes de videovigilància

1.1 Haurà d'existir una relació de proporcionalitat entre la finalitat perseguida i la manera en què es tracten les dades segons el que disposa l'article 4 de la Instrucció 1/2006 de l'AEPD i de la LOPD, respectivament.

1.2 Haurà d'informar-se sobre la captació i/o gravació de les imatges segons establix l'article 3 de la Instrucció 1/2006 de l'AEPD i l'article 5 de la LOPD.

1.3 Atenent el que disposa l'article 4 de la Instrucció 1/2006 de l'AEPD, l'ús d'instal·lacions de càmeres o videocàmeres només serà admissible quan no hi haja un mitjà menys invasiu.

1.4 Segons este mateix article, la instal·lació de sistemes de videovigilància només serà legítima quan servisca per a la finalitat de vigilància i seguretat en el centre educatiu.

1.5 De la mateixa manera, les càmeres i videocàmeres instal·lades en espais privats no podran obtindre imatges d'espais públics.

1.6 Podrien prendre's imatges parcials i limitades de vies públiques quan resulte imprescindible per a la finalitat de vigilància que es pretén, o resulte impossible evitar-ho per raó de la ubicació d'aquelles, atenent el que establix l'article 4 de la Instrucció 1/2006 de l'AEPD.

1.7 L'ús de sistemes de videovigilància haurà de ser respectuós amb els drets de les persones i la resta de l'ordenament jurídic segons establix l'article 5 de la Instrucció 1/2006 de l'AEPD, així com l'article 15 i següents de la LOPD.

1.8 Les imatges es conservaran pel temps imprescindible per a la satisfacció de la finalitat per a la qual es van demanar, com així determina l'article 6 de la Instrucció 1/2006 de l'AEPD.

1.9 Els centres educatius que prenguen la decisió d'instal·lar sistemes de videovigilància en les instal·lacions es faran càrrec del pagament de la instal·lació a càrrec dels pressupostos del centre, i s'ajustaran al que preveu l'Orde de 18 de maig de 1995, per la qual es delega en els directors dels centres educatius no universitaris determinades facultats ordinàries en matèria de contractació i s'aproven les normes que regulen la gestió econòmica dels dits centres (DOCV 09/06/95). Amb relació a este text legal, es recomana la consulta de la norma quarta referida als gastos d'adquisició de mobiliari i equip escolar, així com l'apartat 6 de l'annex III, referent a mobiliari i equip.

1.10 Estos gastos queden condicionats al fet que, prèviament, queden cobertes les necessitats ordinàries per al funcionament normal del centre i que la seua quantia no supere la quantitat fixada en els pressupostos generals de la Generalitat per al corresponent exercici.

2. Principi d'informació

2.1 El director o directora del centre es responsabilitzarà de complir el deure d'informació previst en l'article 3.a) de la Instrucció 1/2006 de l'AEPD, «a) Col·locar, en les zones videovigilades, almenys un distintiu informatiu ubicat en lloc prou visible, tant en espais oberts com tancats». Per a això, s'haurà de col·locar un cartell informatiu en les zones videovigilades (consulteu l'annex II. Models d'informació), tant en recintes tancats com oberts.

2.2 A més, es disposarà d'un imprés en el qual es detalle la informació prevista en l'article 3.b) de la Instrucció 1/2006, «b) Tindre a disposició dels/les interessats/ades impresos en què es detalle la informació prevista en l'article 5.1 de la Llei Orgànica 15/1999». Este imprés estarà disponible de manera visible en el tauler de comunicats del centre per a qualsevol persona de la qual s'haja captat la seua imatge (consulteu l'annex II. Models d'informació).

3.Principis de qualitat, proporcionalitat i finalitat del tractament

3.1 La instal·lació de càmeres de videovigilància en els centres educatius a fi de controlar conductes que puguen afectar la seguretat, ha de ser una mesura proporcional en relació amb la infracció que es pretenga evitar i, en cap cas, ha de suposar el mitjà inicial per a dur a terme funcions de vigilància. La utilització d'estos sistemes ha de ser proporcional al fi perseguit, que en tot cas haurà de ser legítim.

3.2 La instal·lació de càmeres de videovigilància serà una mesura proporcional i justificada atenent el que disposa l'article 4 de la Instrucció 1/2006 de l'AEPD,
« 1. De conformitat amb l'article 4 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, les imatges només seran tractades quan siguen adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, legítimes i explícites, que hagen justificat la instal·lació de les càmeres o videocàmeres. 2. Només es considerarà admissible la instal·lació de càmeres o videocàmeres quan la finalitat de vigilància no puga obtindre's per mitjà d'altres mitjans que, sense exigir esforços desproporcionats, resulten menys intrusius per a la intimitat de les persones i per al seu dret a la protecció de dades de caràcter personal. 3. Les càmeres i videocàmeres instal·lades en espais privats no podran obtindre imatges d'espais públic, llevat que resulte imprescindible per a la finalitat de vigilància que es pretén, o resulte impossible evitar-ho per raó de la ubicació d'aquelles. En tot cas haurà d'evitar-se qualsevol tractament de dades innecessàries per a la finalitat perseguida».

3.3. Els menors són subjectes mereixedors d'una especial protecció, per la qual cosa el principi de proporcionalitat haurà d'aplicar-se amb un rigor extrem. Per a això, en centres educatius, esta mesura només serà legítima quan derive d'una necessitat ineludible, quan la mesura siga la més adequada i sempre que no hi haja una mesura alternativa. En particular:

a) La zona objecte de videovigilància serà la mínima imprescindible i comprendrà espais públics, com ara accessos o corredors.

b) En cap cas podran instal·lar-se estos mitjans en espais protegits pel dret a la intimitat, com ara banys, vestuaris o aquells en què s'exercisquen activitats la captació dels quals puga afectar la imatge o la vida privada.

c) Excepte en circumstàncies excepcionals, no resulta admissible la captació d'imatges amb fins de control d'assistència escolar.

d) L'ús de videocàmeres amb fins de seguretat en espais de recreació, aules i altres àmbits en què es desenrotlla la personalitat dels menors només podran ser objecte de gravació en presència de circumstàncies excepcionals, justificades per la presència d'un risc objectiu i previsible per a la seguretat dels menors.

4. Encarregat del tractament

4.1 La contractació d'empreses de seguretat per a la instal·lació i manteniment del sistema de videovigilància en el centre educatiu públic pot implicar l'accés de l'empresa de seguretat als equips que emmagatzemen o capturen les imatges. Per tant, en estos casos l'empresa de seguretat adquirix la consideració d'encarregat del tractament, la qual cosa implica la subscripció d'un contracte d'accés a les dades per compte de tercers. Per això, segons el que disposa l'article 12 de la LOPD: «1. No es considerarà comunicació de dades l'accés d'un tercer a les dades quan este accés siga necessari per a la prestació d'un servici al responsable del tractament. 2. La realització de tractaments per compte de tercers haurà d'estar regulada en un contracte que haurà de constar per escrit o d'alguna altra manera que permeta acreditar-ne la subscripció i el contingut, i s'establirà expressament que l'encarregat del tractament únicament tractarà les dades d'acord amb les instruccions del responsable del tractament, que no les aplicarà o utilitzarà amb fi diferent del que figure en el dit contracte, ni les comunicarà, ni tan sols per a conservar-les, a altres persones. En el contracte s'estipularan, així mateix, les mesures de seguretat a què es referix l'article 9 d'esta llei que l'encarregat del tractament està obligat a implementar. 3. Una vegada complida la prestació contractual, les dades de caràcter personal hauran de ser destruïdes o tornades al responsable del tractament, igual que qualsevol suport o documents en què conste alguna dada de caràcter personal objecte del tractament. 4. En el cas que l'encarregat del tractament destine les dades a una altra finalitat, les comunique o les utilitze incomplint les estipulacions del contracte, serà considerat, també, responsable del tractament, i respondrà de les infraccions en què haja incorregut personalment».

4.2 L'elaboració i la firma del dit contracte, de compliment obligatori, permetrà involucrar l'empresa de seguretat com a encarregada del tractament, i l'obligarà a adoptar les mesures de seguretat tècniques i organitzatives que garantisquen la seguretat dels tractaments realitzats, corresponents al nivell de seguretat bàsic. Les dites mesures figuren en l'annex III. Mesures de seguretat de nivell bàsic.

4.3. En aquells casos en els quals hi haja una prestació de servicis sense accés a dades personals, haurà de figurar expressament en el contracte de prestació de servicis la prohibició d'accés a dades personals.

5. Mesures de seguretat

5.1 Segons establix l'article 9 de la Instrucció 1/2006 de l'AEPD: «el responsable haurà d'adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades i n'eviten l'alteració, la pèrdua, el tractament o l'accés no autoritzat».

Per tant, el centre educatiu públic haurà d'adoptar les mesures de seguretat de nivell bàsic per al fitxer de videovigilància, de manera que es garantisca també el compliment del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el reglament de desplegament de la llei 15/1999 (d'ara en avant RLOPD).

5.2. En general, els sistemes de videovigilància són tractaments automatitzats, per la qual cosa hauran d'adoptar-se les mesures de nivell bàsic que figuren en el RLOPD, i que figuren en l'annex III. Mesures de seguretat de nivell bàsic i annex IV. Mesures tècniques de seguretat.

6. Cancel·lació de les imatges
6.1 Les imatges hauran de ser cancel·lades una vegada transcorregut el termini d'un mes des de la seua gravació, d'acord amb l'article 6 de la Instrucció 1/2006 de l'AEPD, segons la qual «les dades seran cancel·lades en el termini màxim d'un mes des de la seua captació».

6.2. En aquells casos en què el responsable constate la gravació d'un delicte o d'una infracció administrativa sobre els quals haja de ser informada una autoritat, i la denuncie, haurà de conservar les imatges a disposició de l'esmentada autoritat.

7. Inscripció de fitxers
7.1 Segons l'article 7 de la Instrucció 1/2006 de l'AEPD: «1. La persona o entitat que preveja la creació de fitxers de videovigilància haurà de notificar-ho prèviament a l'Agència Espanyola de Protecció de Dades, per a la seua inscripció en el Registre General d'esta. Tractant-se de fitxers de titularitat pública haurà d'ajustar-se al que establix l'article 20 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. 2. A este efecte, no es considerarà fitxer el tractament consistent exclusivament en la reproducció o emissió d'imatges en temps real».

7.2 La conselleria competent en matèria d'educació és l'encarregada del registre del fitxer de videovigilància en el Registre General de l'AEPD, prèvia publicació de l'ORDE 14/2011, de 7 d'octubre, de la Conselleria d'Educació, Formació i Ocupació, per la qual es crea el fitxer amb dades de caràcter personal de videovigilància.

7.3 La conselleria competent en matèria d'educació disposarà d'un inventari d'aquells centres que instal·len sistemes de videovigilància.

7.4 El centre educatiu haurà de sol·licitar l'autorització/regularització per a la instal·lació del sistema de videovigilància, tal com es descriu en el procediment del punt 8 del present annex.

7.5 En aquells casos en els quals les videocàmeres que s'hagen d'instal·lar reproduïsquen les imatges en temps real (sense gravació ni emmagatzematge d'imatges), únicament estaran subjectes a informar els afectats a través de cartells informatius (vegeu l'annex II. Models d'informació), i no serà obligatòria ni necessària la inscripció del fitxer.

8. Procediment
8.1 El procediment que ha de seguir un centre educatiu que tinga instal·lat prèviament a la publicació d'esta instrucció un sistema de videovigilància en les seues instal·lacions o haja d'instal·lar-lo, és el següent:

8.1.1 Haurà de dirigir una sol·licitud a la direcció territorial competent en matèria d'educació corresponent, i podran presentar-se utilitzant els mitjans telemàtics facilitats pels servidors

d'informació de la conselleria competent en matèria d'educació. El formulari de sol·licitud es troba disponible en l'oficina virtual <https://oficinavirtual.edu.gva.es/oficina_edu/>

8.1.2 Les sol·licituds hauran d'anar acompanyades de la documentació següent:

- Projecte d'instal·lació del sistema de videovigilància previst, indicant si es tracta o no d'una regularització d'instal·lació prèvia.
- Acord favorable del consell escolar.
- Pressupostos d'execució.
- Informe de la unitat tècnica, que supervisarà, així mateix, l'execució de les instal·lacions.
- Informe de necessitat, proporcionalitat i idoneïtat elaborat per la Inspecció Educativa, en què es valorarà l'existència d'una necessitat ineludible per no existir una mesura alternativa i el compliment del punt 3 de la present instrucció.
- Informe tècnic de la Direcció General de Tecnologies de la Informació de la Conselleria d'Hisenda i Administració Pública.

8.1.3 Tota la documentació haurà d'adjuntar-se a l'expedient tramitat telemàticament. La documentació que no complisca estos requisits no serà tinguda en compte a l'hora de tramitar la sol·licitud.

8.1.4 Si la sol·licitud no reunix els requisits i documents que s'assenyalen en estes bases, es requerirà el centre educatiu perquè, en un termini de quinze dies hàbils, esmene la falta o acompanye els documents preceptius, amb la indicació que, en cas de no fer-ho, es tindrà en compte a l'hora de dictar la resolució i es considerarà que desistix de la sol·licitud.

8.1.5 Les dades personals dels representants dels centres educatius, arreplegades en el transcurs del procediment, seran incloses en un fitxer, en els termes i condicions que s'arrepleguen en la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, així com en el Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el reglament de desplegament de l'esmentada llei orgànica.

8.1.6 La instrucció del procediment correspondrà a la direcció territorial competent en matèria d'educació corresponent, la qual realitzarà d'ofici totes actuacions que considere necessàries per a la determinació, coneixement i comprovació de les dades en virtut de les quals ha de formular-se la proposta de resolució.

8.1.7 Una vegada valorat l'expedient, el director territorial corresponent resoldrà l'autorització de les instal·lacions. El termini màxim per a dictar i notificar la resolució corresponent serà de sis mesos a comptar de la data de la presentació de la sol·licitud en la direcció territorial corresponent, de conformitat amb el que establix l'article 42 de la LRJAP.

8.2. Els centres educatius que hagen realitzat la instal·lació de sistemes de videovigilància de manera prèvia a la publicació de la present disposició hauran de presentar la sol·licitud d'autorització en el termini màxim de 6 mesos a partir de la publicació de la present disposició.

8.3. Després de la instal·lació del sistema de videovigilància en el centre educatiu, es podran exercir funcions d'inspecció o control, a fi de supervisar el compliment o no de les mesures de seguretat implantades en el centre educatiu i establides en la present disposició.

9. Modificació de la instal·lació de sistemes de videovigilància en centres educatius
Els centres educatius que realitzen modificacions en els sistemes de videovigilància instal·lats en les seues instal·lacions hauran de notificar-ho a la conselleria competent en matèria d'educació, la qual podrà exercir funcions d'inspecció o control, a fi de supervisar les modificacions realitzades i el seu corresponent compliment o no de les mesures de seguretat establides en la present disposició.

10. Dret d'accés
10.1 Per mitjà del dret d'accés, la persona titular de la imatge o el seu representant legal té dret que la persona responsable del tractament l'informe sobre si la seua imatge ha sigut captada a través de sistemes de videovigilància, la finalitat de la captació, si la imatge és registrada en un fitxer, si és objecte d'algun altre tractament, si s'ha realitzat o s'ha previst alguna comunicació i quin és el període de conservació de les imatges.

10.2 Quan la persona interessada així ho demane, també té dret a accedir a les imatges i a obtindre'n una còpia, com també de les elaboracions posteriors que s'hagen fet.

10.3 En el cas que l'exercici del dret afecte també imatges de terceres persones, llevat que es compte amb el seu consentiment, l'accés requerix la dissociació prèvia de les imatges amb qualsevol mitjà que impedisca la identificació. Quan la dissociació exigisca esforços desproporcionats en atenció al lapse temporal registrat o a l'elevat nombre de terceres persones afectades, la persona responsable pot sol·licitar que es reduïsca el període de gravació a què es pretenga tindre accés.

11. Dret de rectificació
11.1 Només és procedent l'exercici del dret de rectificació de les imatges captades amb sistemes de videovigilància quan la imatge haja sigut distorsionada o alterada després de la captació.

11.2 A fi de complir el que preveu este article, quan s'alteren o distorsionen les imatges s'ha de guardar una còpia de la gravació original o disposar d'un mecanisme de recuperació de la informació original. L'alteració o distorsió ha de quedar reflectida en el registre d'incidències, i s'ha d'indicar el període afectat i el motiu.

12. Dret de cancel·lació
Per mitjà del dret de cancel·lació, la persona titular de la imatge o el seu representant legal pot demanar la supressió, previ bloqueig, de les seues imatges o veu el tractament de les quals siga inadequat, excessiu o contrari a l'ordenament jurídic.

13. Dret d'oposició
Per mitjà del dret d'oposició, a menys que una norma amb rang de llei o norma de dret comunitari d'aplicació directa dispose el contrari, la persona titular de la imatge o el seu representant legal pot demanar l'exclusió del tractament de la seua imatge en aquells supòsits en què no siga necessari el

seu consentiment. La sol·licitud d'exercici d'este dret ha de justificar-se en motius fonamentats i legítims relatius a una situació personal concreta.

14. Procediment d'exercici de drets

14.1 Per a l'exercici dels drets d'accés, rectificació, cancel·lació i oposició, cal formular una sol·licitud dirigida al director del centre docent responsable del fitxer, indicant el lloc, la data i l'hora aproximada, en franges no superiors a dos hores, en què la seua imatge va poder ser captada. La sol·licitud ha d'acompanyar-se d'una imatge de la persona sol·licitant que corresponga al període en què es va captar, de manera que permeta identificar-la. A fi de comprovar la coincidència entre la imatge aportada i les imatges registrades, es poden utilitzar ferramentes de reconeixement d'imatges.

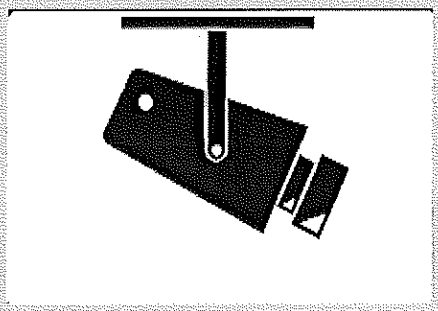
14.2 La tramitació i la resolució de la sol·licitud es regix pel que establixen la normativa de protecció de dades de caràcter personal i per la present instrucció. L'obligació de resoldre persistix, amb independència que les imatges no hagen sigut registrades o que ja hagen sigut cancel·lades en el moment en què s'exercix el dret. En este últim cas, la resolució pot limitar-se a exposar esta circumstància i a informar de la impossibilitat material de donar satisfacció al dret exercit.

14.3. Pot denegar-se la sol·licitud d'exercici dels drets d'accés, rectificació, cancel·lació o oposició quan no concórreguen els requisits exigibles, o quan el nivell de coincidència entre la imatge aportada amb la sol·licitud i les que hagen sigut objecte de tractament no permeta assegurar que esta última correspon a la persona interessada. També pot denegar-se quan no hagen sigut registrades o ja hagen sigut cancel·lades.

ANNEX II

Models d'informació

ZONA VIDEOVIGILADA



LLEI ORGÀNICA 15/1999, DE PROTECCIÓ DE DADES

POT EXERCIR ELS SEUS DRETS DAVANT DE:

□Inseriu el nom del centre docent□

□Inseriu l'adreça del centre docent□

<Inseriu el logo del centre>

CLÀUSULA INFORMATIVA DEL SISTEMA DE VIDEOVIGILÀNCIA

De conformitat amb el que disposa l'article 5.1 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades, s'informa:

1. Que les seues dades personals s'incorporaran al fitxer denominat VIDEOVIGILÀNCIA, del qual és responsable eixe organisme, creat per ORDE 14/2011, de 7 d'octubre, de la Conselleria d'Educació, Formació i Ocupació, per la qual es crea el fitxer amb dades de caràcter personal de videovigilància i/o seran tractats amb la finalitat de seguretat a través d'un sistema de videovigilància.

2. Que el destinatari de les seues dades personals és l'empresa de seguretat <Indiqueu el nom de l'empresa de seguretat, si és procedent>

3. Que pot exercir els seus drets d'accés, cancel·lació i oposició davant del responsable del fitxer.

4. Que el responsable del fitxer de tractament és <Indiqueu el nom o raó social del centre educatiu> ubicat en <Indiqueu l'adreça del centre educatiu>

ANNEX III

Mesures de seguretat de nivell bàsic

1. Funcions i obligacions del personal

2. Les funcions i obligacions de cada un dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació estaran clarament definides i documentades en el document de seguretat.
També es definiran les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.

3. El responsable del fitxer o tractament adoptarà les mesures necessàries perquè el personal conega d'una manera comprensible les normes de seguretat que afecten el desenrotllament de les seues funcions, així com les conseqüències en què puga incórrer en cas d'incompliment.

2. Registre d'incidències

Haurà d'existir un procediment de notificació i gestió de les incidències que afecten les dades de caràcter personal i establir un registre en què es faça constar el tipus d'incidència, el moment en què s'ha produït, o si és el cas, detectat, la persona que realitza la notificació, a qui se li comunica, els efectes que s'hagen derivat d'esta i les mesures correctores aplicades.

3. Control d'accés

1. Els usuaris tindran accés únicament a aquells recursos que necessiten per al desenrotllament de les seues funcions.
2. El responsable del fitxer s'encarregarà que hi haja una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cada un d'ells.
3. El responsable del fitxer establirà mecanismes per a evitar que un usuari puga accedir a recursos amb drets diferents dels autoritzats.
4. Exclusivament, el personal autoritzat per a això en el document de seguretat podrà concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, d'acord amb els criteris establits pel responsable del fitxer.
5. En el cas que hi haja personal alié al responsable del fitxer que tinga accés als recursos haurà d'estar sotmés a les mateixes condicions i obligacions de seguretat que el personal propi.

4. Gestió de suports i documents

1. Els suports i documents que continguen dades de caràcter personal hauran de permetre identificar el tipus d'informació que contenen, ser inventariats, i només hauran de ser accessibles pel personal autoritzat per a això en el document de seguretat.
S'exceptuen estes obligacions quan les característiques físiques del suport n'impossibiliten el compliment, i en quedarà constància motivada en el document de seguretat.
2. L'eixida de suports i documents que continguen dades de caràcter personal, incloent-hi els compresos i/o annexos a un correu electrònic, fora dels locals sota el control del responsable del fitxer o tractament haurà de ser autoritzada pel responsable del fitxer o trobar-se degudament autoritzada en el document de seguretat.

3. En el trasllat de la documentació s'adoptaran les mesures dirigides a evitar la sostracció, pèrdua o accés indegut a la informació durant el seu transport.
4. Sempre que haja de rebutjar-se qualsevol document o suport que continga dades de caràcter personal s'haurà de destruir o esborrar, per mitjà de l'adopció de mesures dirigides a evitar l'accés a la informació continguda en este o la recuperació posterior.
5. La identificació dels suports que continguen dades de caràcter personal que l'organització considere especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permeten als usuaris amb accés autoritzat als esmentats suports i documents identificar-ne el contingut, i que dificulten la identificació per a la resta de persones.

5. Identificació i autenticació
1. El responsable del fitxer o tractament haurà d'adoptar les mesures que garantisquen la correcta identificació i autenticació dels usuaris.
2. El responsable del fitxer o tractament establirà un mecanisme que permeta la identificació de manera inequívoca i personalitzada de tot aquell usuari que intente accedir al sistema d'informació i la verificació que està autoritzat.
3. Quan el mecanisme d'autenticació es base en l'existència de contrasenyes existirà un procediment d'assignació, distribució i emmagatzematge que en garantisca la confidencialitat i integritat.
4. El document de seguretat establirà la periodicitat, que en cap cas serà superior a un any, amb la qual han de ser canviades les contrasenyes que, mentres estiguen vigents, s'emmagatzemaran de manera inintel·ligible.

6. Còpies de suport i recuperació
1. Hauran d'establir-se procediments d'actuació per a la realització, com a mínim setmanal, de còpies de suport, llevat que en el dit període no s'haja produït cap actualització de les dades.
2. Així mateix, s'establiran procediments per a la recuperació de les dades que garantisquen en tot moment la seua reconstrucció en l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció.
Únicament, en el cas que la pèrdua o destrucció afecte fitxers o tractaments parcialment automatitzats, i sempre que l'existència de documentació permeta aconseguir l'objectiu a què es referix el paràgraf anterior, s'haurà de procedir a gravar manualment les dades, i quedarà constància motivada d'este fet en el document de seguretat.
3. El responsable del fitxer s'encarregarà de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de suport i de recuperació de les dades.
4. Les proves anteriors a la implantació o modificació dels sistemes d'informació que tracten fitxers amb dades de caràcter personal no es realitzaran amb dades reals, llevat que s'assegure el nivell de seguretat corresponent al tractament realitzat i s'anote la seua realització en el document de seguretat.
Si està previst realitzar proves amb dades reals, prèviament haurà d'haver-se realitzat una còpia de seguretat.

ANNEX IV

Mesures tècniques de seguretat

1. Compliment de mesures tècniques de seguretat addicionals

2. La transmissió de dades de caràcter personal a través de xarxes cablejades o xarxes sense fil de comunicació electròniques es realitzarà xifrant estes dades, o bé, utilitzant qualsevol altre mecanisme que garantisca que la informació no siga intel·ligible ni manipulada per tercers.

3. Per al xifratge de les comunicacions s'utilitzaran protocols criptogràfics que proporcionen la seguretat de la informació que viatja a través d'estes, emprant algoritmes d'encriptació actuals.

4. L'accés a la sala on es troben els equips físics en els quals s'emmagatzemen les imatges hauran de disposar de mecanismes de seguretat que impedisquen l'accés no autoritzat de persones alienes o no autoritzades.

5. Les xarxes de comunicació electròniques per a la transmissió d'imatges dels dispositius de videovigilància, en cap cas podran ser les xarxes de comunicacions de dades corporatives dels centres educatius, i serà responsabilitat de l'empresa instal·ladora l'ús d'una xarxa pròpia independent de les existents en el centre.