Ajuntament de
Cerdanyola del Vallès

Pl. Francesc Layret, s/n
08290 Cerdanyola del Vallès
Barcelona
Telèfon 93 580 88 88
Fax 93 580 16 20
www.cerdanyola.cat

REGLAMENT INTERN PER A LA PROTECCIÓ DE LES DADES DE CARÀCTER PERSONAL DE L'AJUNTAMENT DE CERDANYOLA DEL VALLÈS

ÍNDEX

Exposició de motius

SOBRE L'APROVACIÓ DEL REGLAMENT INTERN PER A LA PROTECCIÓ DE LES DADES DE CARÀCTER PERSONAL DE L'AJUNTAMENT DE CERDANYOLA DEL VALLÈS.

El Butlletí Oficial de l'Estat núm. 17, de 19 de gener de 2008, publicava el *Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (RPDP). La seva entrada en vigor es produí el 19 d'abril de 2008.

La llei orgànica de protecció de dades de caràcter personal nasqué amb una àmplia vocació de generalitat, ja que el seu article primer, en determinar el seu objecte, fixa que pretén garantir i protegir, pel que fa al tractament de les dades de caràcter personal, les llibertats públiques i els drets fonamentals de les persones físiques i, especialment, del seu honor i intimitat personal i familiar. I, de conformitat amb el seu article 2, que fixa l'àmbit d'aplicació, comprèn el tractament automatitzat i el no automatitzat de les dades de caràcter personal. No obstant això, en la seva disposició addicional primera determinava que en el supòsit de fitxers i tractaments no automatitzats, l'adequació a la LOPD s'havia de fer en el termini de dotze anys a comptar des del 24 d'octubre de 1995; per tant, es diferia l'aplicació integra de la llei, per als fitxers no automatitzats, al 24 d'octubre de 2007.

La LOPD es considerà desenvolupada, de manera parcial, pel *Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal* i pel *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal*. Destacarem que aquesta normativa reglamentària no resultava aplicable als fitxers que continguin dades de caràcter personal però que no tinguin un suport informàtic.

El ja citat RPDP, com s'ha dit, comprèn en el seu àmbit d'aplicació totes les dades de caràcter personal registrades en suport físic que les faci susceptibles de tractament i tota modalitat d'ús posterior d'aquestes dades pels sectors públic i privat. Bona part del seu contingut s'aplica als fitxers no automatitzats, tal i com es determina en el Capítol IV.

La Disposició transitòria segona fixa els terminis d'implantació de les mesures de seguretat regulades en el reglament. Si bé, pel que fa a les mesures de seguretat dels fitxers automatitzats, majoritàriament, es tractarà de regular normativament l'aplicació que ja s'ha fet del *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados de Datos de Carácter Personal*, no succeeix el mateix amb els fitxers no

automatitzats, respecte dels quals no tenim formalment implantades les mesures de seguretat que deriven de la LOPD. Per a aquests, el RPDP determina que les mesures de seguretat —dels fitxers ja creats— han d'implantar-se en el termini d'un any, divuit mesos o dos anys des de l'entrada en vigor del Reglament, segons el seu nivell de protecció sigui bàsic, mitjà o alt.

Pretén, en conseqüència, aquest reglament, determinar les mesures de seguretat que han d'ésser implantades, i regular formalment les ja implantades, que facin efectiva la protecció de dades de caràcter personal en l'actuació de l'Ajuntament de Cerdanyola del Vallès, tant pel que fa als fitxers automatitzats com a fitxers en suport diferent a l'electrònic.

Estableix aquest reglament, doncs, a regular el conjunt de mesures de seguretat a adoptar per la persona responsable de cada fitxer i per la persona encarregada del seu tractament, sempre que es tractin dades de caràcter personal.

Aquestes mesures, bàsicament, són de caràcter organitzatiu, destinades a establir els procediments, les normes, les regles i els estàndards d'aplicació que garanteixin la seguretat; i d'abast tècnic, destinades, principalment, a conservar la integritat física de la informació, per tal d'evitar robatoris, pèrdues o alteracions no justificades. S'hi inclou, com no pot ser d'altra manera, les mesures de seguretat referents als locals on emmagatzemem les dades i els continents que els suporten, com ara els armaris, els arxivadors, els ordinadors o els servidors, entre d'altres.

En relació directa als Sistemes d'Informació de l'Ajuntament de Cerdanyola del Vallès, en aquest Reglament es recullen les prescripcions que ha d'observar-ne tota persona usuària o amb accés a les dades personals incloses als fitxers municipals. En aquest sentit, cal deixar constància del fet que vàries d'aquestes normes d'ús ja estaven fixades, per bé que amb el Reglament s'inclouen en un text únic i sistematitzat, la qual cosa ha de facilitar el seu coneixement i observança.

En aquesta línia, ha de destacar-se l'aprovació de la *Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, que ha de facilitar i comportar un ús majoritàriament progressiu de les tecnologies electròniques, el que implica una preocupació major per la protecció de dades. Així ho ha reconegut el legislador en l'exposició de motius de l'esmentada norma, quan diu:

> *«El reconocimiento general del derecho de acceder electrónicamente a las Administraciones Públicas tiene otras muchas consecuencias a las que hay que dar solución y de las que aquí, de forma resumida, se enumeran algunas.*
> *Así, en primer lugar, la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo*

expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración.»

L'esmentada llei 11/2007, es refereix, específicament, a la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* en l'article 4, en regular els *principis generals* en la utilització de les tecnologies de la informació, quan determina el respecte al dret a la protecció de dades de caràcter personal. També en l'article 6.2.*b),* quan es refereix als *drets de la ciutadania*, pel que fa al dret de no aportar dades i documents que ja estiguin en poder de l'Administració, el que obliga les administracions públiques a obtenir aquestes dades per mitjans electrònics. I, en línia amb aquest precepte, l'article 9, de les *transmissions de dades entre administracions públiques*, que fixa, per a un eficaç exercici del dret reconegut en l'apartat 6.2.*b),* que cada Administració haurà de facilitar l'accés de la resta d'administracions públiques a les dades relatives a les persones interessades de què disposin i que es trobin en suport electrònic, amb acompliment estricte de la LOPD i la seva normativa de desenvolupament. També s'hi refereix l'article 27, de *les comunicacions electròniques*, que en el seu apartat 5è determina que els requisits de seguretat i integritat de les comunicacions s'establirà de forma apropiada al caràcter de les dades objecte de comunicació, d'acord amb criteris de proporcionalitat i conformement a la legislació vigent en matèria de protecció de dades de caràcter personal. Destaquem, igualment, l'article 31, que es dedica a l'*arxiu electrònic de documents* i que determina que els mitjans o els suports en què s'emmagatzemin documents hauran de comptar amb mesures de seguretat que garanteixin la integritat, l'autenticitat, la confidencialitat, la qualitat, la protecció i la conservació dels documents emmagatzemats i, en particular, asseguraran la identificació de les persones usuàries i el control d'accessos, així com l'acompliment de les garanties previstes en la legislació de protecció de dades. Finalment, hem de ressaltar el contingut de la disposició addicional segona de la llei, que es refereix a la *formació dels empleats públics*, tot i que el seu àmbit queda restringit a l'Administració General de l'Estat, però hem d'afirmar la necessitat ineludible d'aplicar-la a qualsevol Administració Pública, atès que determina l'obligació de l'Administració de promoure la formació del personal al seu servei en la utilització dels mitjans electrònics per al desenvolupament de les activitats que li són pròpies i, en especial, fixa que els empleats públics rebran formació específica que garanteixi els coneixements actualitzats de les condicions de seguretat de la utilització de mitjans electrònics en l'activitat administrativa, així com de protecció de les dades de caràcter personal, respecte a la propietat intel·lectual i industrial i gestió de la informació.

Per tant, són destinatàries de les prescripcions del Reglament totes les persones usuàries dels Sistemes d'Informació de l'Ajuntament de Cerdanyola, condició que inclou el personal que hi presta servei i també les persones col·laboradores que els utilitzin.

El Reglament Intern conté, en síntesi, previsions i prescripcions sobre:

→ La titularitat i la propietat corporativa dels equips, els recursos i els sistemes informàtics, així com de la necessitat de fer-ne un ús acurat dintre de les tasques associades a cada lloc de treball.
→ L'ús del programari sobre la base de les condicions de legalitat, actualització i compatibilitat.
→ La necessitat d'estalviar en el consum dels recursos informàtics per tal de millorar el grau d'eficiència i en benefici del medi ambient.
→ Protecció de les xarxes informàtiques i de telecomunicacions corporatives.
→ Utilització de les eines informàtiques i de telecomunicacions en l'àmbit exclusiu de l'entorn de treball.
→ Responsabilitats d'empleats/empleades i persones col·laboradores de l'Ajuntament en relació amb els recursos informàtics i de telecomunicacions assignats o encomanats.
→ Utilització del correu electrònic.
→ Límits, condicions i obligacions que s'han d'observar en relació amb el tractament de dades de caràcter personal

Es tracta, per tant, d'establir, en un instrument normatiu, el conjunt de polítiques de seguretat respecte de les dades personals que emprem en l'exercici de les competències locals; per tal de garantir-ne la confidencialitat, la integritat i la disponibilitat de la informació.

ANTECEDENTS

L'article 18.4 de la Constitució Espanyola de 1978 estableix la necessitat de limitar l'ús de la informàtica per garantir l'honor, la intimitat personal i familiar i la pròpia imatge, així com el legítim exercici dels drets pels ciutadans i per les ciutadanes.

La *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, en vigor des del 14 de gener de 2000, ha vingut a regular, entre d'altres aspectes, la garantia de la seguretat de les dades de caràcter personal, per evitar-ne la seva alteració, la pèrdua o el tractament o accés no autoritzat.

El *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal*, té com a objecte l'establiment de les mesures tècniques i organitzatives necessàries per garantir la seguretat que han de reunir els fitxers automatitzats i no automatitzats, els centres de tractament, els locals, els equips, els sistemes, els programes i les persones que intervinguin en el tractament de les dades de caràcter personal subjectes a la LOPD.

El sistema d'informació municipal integra documentació, elements de maquinari, programari, elements de comunicació i tots aquells dispositius que permetin el tractament de la informació, i conté diferents fitxers subjectes a la reglamentació i limitacions d'ús establerts a la LOPD.

El reglament estatal prescriu l'elaboració d'un document de funcions i obligacions que contingui les previsions establertes i que sigui àmpliament conegut pel personal al servei de l'Administració que tingui, o pugui tenir, accés a qualsevol de les informacions, fitxers o elements indicats.

Reglament intern per a la protecció de les dades de caràcter personal de l'Ajuntament de Cerdanyola del Vallès.

TÍTOL I. DISPOSICIONS GENERALS

Article 1. **Objecte**
Constitueix objecte d'aquest reglament establir les mesures tècniques i organitzatives necessàries per a la regulació del sistema de seguretat dels recursos físics i lògics que es trobin ubicats a qualsevol edifici o dependència de gestió municipal o adscrit als serveis que presta l'Ajuntament de Cerdanyola del Vallès i que permetin el tractament de la informació de caràcter personal.

Article 2. **Àmbit d'aplicació**
Aquest reglament serà d'aplicació a les dades de caràcter personal registrades en suport físic, susceptibles de tractament, i a tota modalitat d'ús posterior d'aquestes dades, que es faci per part de l'Ajuntament de Cerdanyola del Vallès, sigui directament per part del seu personal o a través de terceres persones.
Queda exclòs del seu àmbit d'aplicació el tractament de les dades que la normativa estatal sobre protecció de dades no inclogui.
Especialment, les mesures de seguretat regulades per aquest Reglament seran d'aplicació al tractament de les dades persones que es trobin en els fitxers inclosos en l'*Inventari de Fitxers Corporatius i temporals*[1] (en endavant, els *Fitxers*) i, específicament, en aquells declarats davant l'Agència de Protecció de Dades competent.
Es regiran pels articles especialment previstos en aquest Reglament els centres de tractament, locals, equips, sistemes, programes i les persones que intervinguin en el tractament automatitzat o no de les dades de caràcter personal.

Article 3. **Definicions**
Sense perjudici de les definicions que conté la normativa estatal, als efectes establerts en aquest reglament, s'entendrà per:

a) *Administradors de Sistemes i de Bases de Dades*: Persones encarregades d'administrar les bases de dades corporatives així com de mantenir l'entorn operatiu dels Fitxers.
b) *Arxiu*: L'organisme o la institució des d'on es fan específicament funcions d'organització, de tutela, de gestió, de descripció, de conservació i de difusió de

[1] S'hi incorpora, com a ANNEX 1, l'*Inventari de fitxers corporatius i temporals* (codi PDPL05).

documents i fons documentals. També s'entén per arxiu el fons o el conjunt de fons documentals.

c) *Fitxer corporatiu*: Fitxer en què la seva estructura, finalitat i usos previstos han estat definits sota un sistema de gestió corporatiu i on la finalitat del qual reflecteix el funcionament i les competències municipals.
d) *Fitxer departamental*: Fitxer creat sota la responsabilitat de la persona responsable de cada Servei, d'acord amb les normes organitzatives establertes, en què és competència del Servei decidir sobre tots els aspectes de la gestió i del tractament que se'n faci.
e) *«Freeware»*: Classe de programa totalment gratuït encara que generalment el seu codi no està disponible (també conegut com a codi tancat).
f) *Gestió d'incidències*: Operacions de manteniment d'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 identificació de les persones responsables d'aquests.
g) *Informació*: En sentit general, conjunt organitzat de dades que constitueixen un missatge sobre un determinat ens o fenomen. Segons un altre punt de vista, la informació és un fenomen que proporciona significat o sentit a les coses i indica, mitjançant codis i conjunts de dades, els models del pensament humà.
h) *Llocs de treball*: Tots aquells dispositius des dels quals es pot accedir a les dades dels Fitxers com, per exemple, terminals o ordinadors personals.
Es consideren també llocs de treball aquells terminals d'administració del sistema, com, per exemple, les consoles d'operació, on en alguns casos també poden aparèixer les dades protegides dels sistemes d'informació corporatius.
i) *Seguretat d'informació*: Estableix les normes vàlides, a tota l'organització, sobre com s'ha d'usar la informació i els sistemes d'informació. Així mateix, evita la pèrdua i falsificació de dades, garanteix que les dades estiguin al dia i que la informació es distribueixi sense problemes, amb millora de la qualitat i de l'eficiència dels processos.
j) *«Shareware»*: Classe de software o programes per poder avaluar de forma gratuïta però per un temps, per a un ús o per a característiques limitades. Per adquirir el software de manera completa es necessita procedir a un pagament econòmic (moltes vegades modest).
k) *Sistema Informàtic o aplicacions d'accés als fitxers corporatius*: Tots aquells sistemes informàtics, programes o aplicacions amb els que es pot accedir a les dades dels sistemes d'informació i que són usualment utilitzats pels usuaris per accedir-hi. Aquests sistemes poden ser aplicacions informàtiques expressament dissenyades per accedir als Fitxers o sistemes preprogramats d'ús general com aplicacions o paquets disponibles en el mercat informàtic.

Article 4. **Delegació de competències i funcions**

Es delega en la Junta de Govern Local, o òrgan que legalment la substitueixi, les revisions i les adequacions dels documents annexos a aquest reglament, sempre i

quan no comportin una modificació substancial del seu contingut; amb la finalitat de garantir, en tot moment, que l'activitat administrativa s'adequa a les disposicions vigents en matèria de seguretat de les dades. S'entendrà que no es tracta de modificacions substancials quan les modificacions que s'introdueixin en els documents annexos no s'oposin, contradiguin o vulnerin allò establert en aquest Reglament. En tot cas, de les modificacions que s'introdueixin en els annexos, caldrà donar-ne compte al Ple.

Article 5. **Persones responsables dels Fitxers**

L'Alcaldia-Presidència de l'Ajuntament de Cerdanyola del Vallès és l'òrgan responsable dels Fitxers que contenen la informació municipal i que han estat degudament inscrits davant l'Agència Catalana de Protecció de Dades.

Llevat que altra cosa es determini per l'Alcaldia en exercici de les seves competències, correspondrà a la regidoria sobre la qual recaigui la direcció i la gestió dels Sistemes d'Informació, la direcció interna, l'impuls i la inspecció d'allò que es determina en aquest Reglament i l'elevació de les propostes de resolucions i acords que correspongui adoptar als diferents òrgans de govern municipal.

Per resolució d'alcaldia, prèvia tramitació del procediment de *Nomenament de càrrecs*[2], es designaran les persones o els càrrecs sobre què recauen les diferents funcions en el procediment de tractament de les dades: Encarregats/des del Tractaments que es duen a terme a cada àmbit material d'acord amb l'organigrama en cada moment vigent, Responsable de Seguretat, Administradors/res de Sistemes i Bases de Dades. També es designaran les persones substitutes que hauran d'assumir les funcions en cas d'absència del titular.

També per resolució d'alcaldia, es farà l'assignació de responsabilitats, de tal manera que s'enumerin i actualitzin les obligacions que corresponen a cadascuna de les persones o càrrecs a qui ha conferit les responsabilitats mitjançant el nomenament de càrrecs, en el marc d'allò que determina aquest reglament.

Article 6. **Funcions del Responsable dels Fitxers**

Correspon a l'alcaldia-presidència de l'Ajuntament de Cerdanyola del Vallès, sense perjudici de la seva delegació, adoptar les resolucions relatives a les actuacions en matèria de seguretat de la informació municipal, aquelles que estableix la normativa sectorial i, en especial, les que tot seguit es relacionen:

a) Elaborar, de conformitat amb les directrius establertes en aquest Reglament, el o els documents de seguretat a què es refereix el reglament estatal de la llei de protecció de dades, sense perjudici que es pugui considerar aquest Reglament com a document de seguretat general, als efectes establerts en el reglament estatal de protecció de dades de caràcter personal.

b) Nomenar, mitjançant resolució, les persones responsables de Seguretat, les persones encarregades del Tractament que es duu a terme a cada a cada àmbit

[2] S'hi incorpora, com a ANNEX 2, el procediment de *Nomenament de càrrecs* (codi PDPR01).

material d'acord amb l'organigrama en cada moment vigent i els/les Administradors/res de Sistemes i Bases de Dades.

c) Adoptar les mesures necessàries perquè el personal al servei de l'Ajuntament de Cerdanyola del Vallès conegui les normes de seguretat que afectin el desenvolupament de les seves funcions, així com les responsabilitats en què poden incórrer en cas d'incompliment.

d) Garantir la difusió del Reglament i la resta de procediments, instruccions i plantilles que l'implementen, promoure la seva actualització sempre que es produeixin canvis rellevants en el sistema d'informació o en la manera en què estigui organitzat el tractament de les dades.

e) Garantir l'adequació, en tot moment, del contingut d'aquest Reglament a les disposicions vigents en matèria de protecció de dades, per a la qual cosa proposarà la seva modificació quan sigui necessari.

f) Mantenir una relació actualitzada de les persones usuàries que tinguin accés autoritzat al Sistema d'Informació i recollir-ho a les aplicacions informàtiques corresponents.

g) Establir procediments d'identificació i autenticació per a l'accés al sistema d'informació.

h) Establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de tot aquella persona usuària que intenti accedir al sistema d'informació i la verificació de què està autoritzat.

i) Autoritzar, per escrit, l'execució dels procediments de recuperació de dades.

j) Autoritzar expressament l'execució del tractament de dades de caràcter personal fora dels locals on estan ubicats els Fitxers.

k) Adoptar les mesures correctores a partir de les conclusions extretes, per part del Responsable de Seguretat, de les auditories que es realitzin.

l) Establir els criteris per autoritzar les extraccions de dades del departament cap a l'Arxiu Municipal.

m) Establir els criteris per autoritzar els accessos a les dades de l'Arxiu Municipal.

n) Donar constància motivada dels casos en què per les característiques físiques d'un suport no es puguin complir les obligacions relacionades amb la seva identificació mitjançant l'etiquetatge.

o) Donar constància motivada dels casos en què no sigui possible el xifrat de les dades de nivell alt i el tractament de les quals s'hagi de realitzar necessàriament des d'un dispositiu portàtil.

p) Verificar la correcta definició, funcionament i aplicació dels procediments de realització de còpies de recolzament i recuperació de dades.

q) Establir els criteris per resoldre i donar resposta a les sol·licituds dels diferents procediments habilitats.

Article 7. **Responsables de Seguretat: la Comissió de Seguretat**
Es crea una Comissió de Seguretat que assumirà les funcions que la normativa estatal reserva per al responsable de seguretat, la composició de la qual es determinarà per la Junta de Govern Local, que n'haurà de donar compte al Ple.
La Comissió de seguretat tindrà una composició interdisciplinària, en la qual s'integraran, com a mínim, persones dels àmbits jurídic i informàtic**.**
Les persones que en formin part han de tenir els coneixements tècnics suficients per al desenvolupament de les seves funcions.
L'alcaldia designarà les persones que integraran la comissió de seguretat, i, entre elles, qui n'assumirà la presidència.

Article 8. **Funcions de la Comissió de Seguretat**
Són funcions de la Comissió de Seguretat, en matèria de seguretat de la informació municipal, aquelles que estableix la normativa sectorial i en especial les que tot seguit es relacionen:
a) Proposar, al Responsable dels Fitxers, les actuacions recollides a l'article 6 d'aquest Reglament, a excepció de la de la lletra b).
b) Coordinar la posada en marxa de les mesures establertes en aquest Reglament.
c) Col·laborar amb el Responsable dels Fitxers en la difusió d'aquest Reglament i en el control i l'acompliment de les mesures de seguretat.
d) Analitzar les incidències registrades i prendre les mesures adients en col·laboració del Responsable dels Fitxers.
e) Elaborar semestralment un informe de les revisions realitzades i dels problemes detectats.
f) Analitzar els informes d'Auditoria i elevar les conclusions al Responsable dels Fitxers, o a qui delegui, per a l'adopció de les mesures correctores adequades.
g) Coordinar i fer-ne el seguiment de l'actuació de les persones responsables o encarregades del tractament.
h) Detectar i establir-ne un registre dels fitxers que continguin dades de caràcter personal i que no estiguin en suport electrònic.

Article 9. **Funcions de la Presidència de la Comissió de Seguretat**
Són funcions de la Presidència de la Comissió de Seguretat, en matèria de seguretat de la informació municipal, les que tot seguit es relacionen:
a) Habilitar un Registre d'Incidències, a disposició de totes les persones usuàries i administradors dels Fitxers, perquè s'hi enregistri qualsevol incidència que pugui suposar un perill per a la seguretat dels Fitxers.
b) Habilitar i gestionar un inventari de suports i un Registre d'entrades i sortides de suports, que continguin dades de caràcter personal fora de l'àmbit físic de l'Ajuntament.
c) Verificar la definició i correcta aplicació dels procediments de realització de còpies de recolzament i recuperació de les dades.

d) Revisar periòdicament la informació de control registrada. A aquests efectes, confeccionarà, amb periodicitat mensual, un informe de situació.
e) Controlar, de forma directa, els mecanismes que permetin el registre de les dades d'accés sense permetre la desactivació dels mateixos.
f) Dirigir l'acció de la persona Administradora de Sistemes i de Bases de Dades.

Article 10. **Funcions de la persona Administradora de Sistemes i de Bases de Dades**

Són funcions de la persona Administradora de Sistemes i de Bases de Dades en matèria de seguretat de la informació municipal aquelles que garanteixin la seguretat de les dades que es processen a l'Ajuntament de Cerdanyola del Vallès i, en especial i sense perjudici de la normativa sectorial, les que tot seguit es relacionen:

a) Proposar estàndards i procediments relacionats amb la seguretat.
b) Desenvolupar els plans de seguretat.
c) Gestionar els perfils de les persones usuàries dels sistemes informàtics i els accessos de cadascuna.
d) Controlar i realitzar el seguiment de la seguretat física i lògica de l'entorn informàtic.
e) Proposar, d'acord amb el Responsable dels Fitxers, la classificació de les dades i, en coordinació amb les persones usuàries, les de les aplicacions.
f) Donar suport a les persones usuàries en matèria de seguretat.
g) Avaluar els riscos.
h) Implantar equips, dispositius i paquets relacionats amb la seguretat física i lògica.

La concreció de les funcions que s'assignin a l'Administradora de Sistemes i de Bases de Dades es farà per l'alcaldia, o persona en qui delegui, a proposta de la Comissió de seguretat.

Article 11. **Funcions de les persones encarregades del tractament**

Al efectes establerts en aquest reglament, seran considerats persones encarregades del Tractament que es duu a terme a cada àmbit material, la persona designada per l'alcaldia, d'acord amb l'organigrama vigent en cada moment.

A proposta de la Comissió de Seguiment, l'alcaldia determinarà el nivell orgànic en què recaurà la designació de la persona encarregada del tractament, que serà el/la cap corresponent.

Les funcions atribuïdes a les persones encarregades del tractament aquelles que estableix la normativa sectorial i en especial les que tot seguit es relacionen:

a) Tractar les dades per compte del Responsable dels Fitxers.
b) Sol·licitar l'accés al sistema informàtic per al personal de la unitat administrativa que vulgui accedir fora de la jornada habitual de treball.
c) Relacionar els fitxers de prova amb dades reals i fer-los constar a l'inventari de fitxers corporatius i temporals.

d) Sol·licitar l'accés a les dades, recursos, aplicacions, assignacions de claus d'identificació, etc., que el personal de la unitat administrativa requereixi per al desenvolupament de les seves funcions.
e) Sol·licitar la modificació de privilegis d'accés assignats a les persones usuàries.
f) Enregistrar els fitxers temporals així com donar-los de baixa, segons convingui en cada moment, de l'Inventari de fitxers corporatius i temporals.
g) Informar de la creació, modificació o eliminació de fitxers corporatius.
h) Habilitar els mitjans a través dels quals els formularis de captació de dades disposin del dret d'informació a peu de pàgina.
i) Procedir a activar els mecanismes que permetin regularitzar les dades.
j) Assegurar que tots els tractaments amb tercers, que estan sota l'empara del règim de contractació, siguin adientment formalitzats segons els models que hi ha disponibles.
k) Autoritzar les extraccions de dades del departament cap a l'Arxiu Municipal.
l) Autoritzar els accessos a les dades de l'Arxiu Municipal.
m) Autoritzar la realització de còpies o la reproducció de documentació que contingui dades de caràcter personal.
n) Resoldre i donar resposta a les sol·licituds dels diferents procediments habilitats.
o) Garantirà que els dispositius d'emmagatzematge dels fitxers no automatitzats s'ajustin a allò establert en aquest Reglament i en la normativa sobre protecció de dades de caràcter personal.

Article 12. **Especificació detallada dels recursos objecte de protecció**

Els recursos protegits es divideixen en recursos físics i recursos lògics.
Són recursos físics i estaran protegits els següents:
a) Els centres de tractament i locals on es trobin ubicats els Fitxers o s'emmagatzemin els suports que els continguin[3].
b) Els equips informàtics i els llocs de treball des que es pot tenir accés als Fitxers i que permetin emmagatzemar i processar informació susceptible d'estar sotmesa a la protecció de la LOPD. La informació sobre la relació d'aquests llocs de treball ha de poder obtenir-se mitjançant les aplicacions informàtiques de l'Ajuntament de Cerdanyola del Vallès
c) Els equips informàtics i de comunicacions integrats en la Xarxa Corporativa o en xarxes departamentals, així com l'entorn de sistema operatiu i de comunicacions[4].

[3] S'hi incorpora, com a ANNEX 3, el document que conté la descripció dels recursos físics, identificat com a *Locals i equipaments amb Fitxers o suports que els guarden* (codi PDPL12).

[4] S'hi incorpora, com a ANNEX 4, el document que conté la descripció dels equips informàtics integrats en la xarxa corporativa o en xarxes departamentals i l'entorn operatiu, identificat com a *Entorn de sistema operatiu i de comunicacions dels Fitxer*s (codi PDPL11).

Seran objecte de mesures especials de protecció, com ara les referents a seguretat física, perimetral i la resta relacionades, els servidors corporatius, els dispositius d'emmagatzematge massiu d'informació, els dispositius de telecomunicacions i la infraestructura de xarxa.
Són recursos lògics i estaran protegits els següents:

a) Els sistemes informàtics corporatius o aplicacions per accedir a les dades[5].
b) Estaran igualment subjectes a especial protecció, les taules i Fitxers que tractin dades de caràcter personal, que es creïn amb posterioritat a l'entrada en vigor d'aquest Reglament.
c) Les diferents bases de dades departamentals, en general, i totes aquelles que emmagatzemin dades d'identificació personal de qualsevol tipus.
d) L'accés als recursos de programari disponibles a la xarxa corporativa.
e) El programari d'accés a dades, executable des de qualsevol ordinador personal.
f) L'accés i utilització d'informació procedent de l'exterior via Internet.

TÍTOL II. FUNCIONS I OBLIGACIONS DEL PERSONAL

Article 13. **Subjectes obligats al compliment de la norma**

Aquesta norma és d'obligat compliment pel personal al servei de l'Ajuntament i per tota persona, amb independència de la seva relació laboral o administrativa amb l'Ajuntament de Cerdanyola del Vallès, que per qualsevol mitjà tingui accés a les dades automatitzades, o no, de caràcter personal i als sistemes d'informació que les tracten.
Les responsabilitats disciplinàries, administratives, penals i civils derivades de l'incompliment de les normes indicades en aquest Reglament i en la normativa estatal i autonòmica sobre protecció de dades de caràcter personal s'exigiran de conformitat amb la normativa aplicable sobre la funció pública i sense perjudici d'allò que es disposa als articles 16, 17 i 18 d'aquest Reglament.
A més a més, les persones Administradores de Sistemes i de Bases de Dades hauran de respectar allò que es disposa que es disposa als procediments de control d'accessos, suport i recuperació i gestió[6].

[5] S'hi incorpora, com a ANNEX 5, el document que conté la descripció dels sistemes informàtics corporatius o aplicacions per accedir a les dades, identificat com a *Descripció del sistema informàtic d'accés als Fitxers* (codi PDPL10).

[6] S'hi incorpora, com a ANNEX 6, el document que conté la descripció dels procediments de control d'accessos, suport i recuperació i gestió, identificat com a *Procediments de control d'accessos, suport i recuperació i gestió* (codi PDPL14).

L'obtenció de l'aprovació d'un servei o tasca demandat, excepte en aquells casos en què s'indica la necessitat de l'autorització expressa per part d'alguna de les figures de responsabilitat establertes, s'entendrà vàlida si es fa per mitjà de l'enviament d'un correu electrònic.

Article 14. **Deure de secret i reserva**

Qualsevol persona que intervingui en qualsevol fase del tractament de les dades de caràcter personal està obligada al secret professional i a la reserva professional respecte de les mateixes i al deure de guardar-les, obligacions que subsistiran fins i tot amb posterioritat de l'extinció de la seva relació amb el Responsable dels Fitxers.

En relació a les dades conegudes, no protegides pel secret professional, es procedirà a actuar amb la reserva necessària.

Article 15. **Adopció de mesures necessàries per al coneixement de les normes de seguretat pel personal al servei de l'Ajuntament**

L'alcaldia, com a responsable dels fitxers, a proposta de la Comissió de Seguretat, procedirà a adoptar les mesures necessàries per tal que el personal conegui les normes de seguretat que afecten el desenvolupament de les seves funcions i les responsabilitat en què poden incórrer en cas d'incompliment.

Les persones que actualment presten serveis a l'Ajuntament tindran a la seva disposició, a través de la intranet municipal, l'accés a aquest Reglament i a la documentació que el desplega.

Les persones que entrin a prestar serveis a l'Ajuntament, amb caràcter temporal o permanent rebran còpia d'aquest Reglament al temps de signar el contracte de treball, contracte administratiu o acta de presa de possessió.

Sempre que sigui necessari, degut a canvis en el present Reglament o a la normativa que el desplega, es remetrà, elaborada per la Comissió de Seguretat, una circular informativa, que farà esment de les modificacions produïdes en relació a les matèries regulades per aquest Reglament i/o als procediments, a les instruccions i a les plantilles que el complementen, sense perjudici d'allò que s'estableix respecte dels resultats de les auditories.

Article 16. **Responsabilitat disciplinària**

L'incompliment de l'obligació de secret professional i el deure de guardar-lo, per part del personal al servei de l'Ajuntament, serà sancionat disciplinàriament, prèvia instrucció del preceptiu expedient, com a falta, amb la qualificació que en cada moment determini la normativa aplicable.

Article 17. **Responsabilitat administrativa**

Sens perjudici de la responsabilitat disciplinària en què pugui incórrer el personal al servei de l'Ajuntament, s'exigirà la corresponent responsabilitat patrimonial, en els termes establerts en l'article 145 de la *Ley 30/1992, de 26 de noviembre, de*

Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Article 18. **Responsabilitat penal i civil**
La responsabilitat penal i la responsabilitat civil derivada de delicte en què hagi incorregut el personal al servei de l'Ajuntament, s'exigirà de conformitat amb la legislació corresponent.

TÍTOL III. MESURES, NORMES, PROCEDIMENTS, REGLES I ESTÀNDARDS GARANTS DE LA SEGURETAT DE LA INFORMACIÓ MUNICIPAL

CAPÍTOL I. CONTROL DE SEGURETAT

Article 19. **Control d'accés físic als locals**
Els locals on s'ubiquen els ordinadors que contenen Fitxers amb dades de caràcter personal han de ser objecte d'especial protecció per tal de garantir la disponibilitat i confidencialitat de les dades protegides, especialment en el cas que els Fitxers estiguin ubicats en un servidor accedit a través d'una xarxa, i hauran de disposar dels mitjans mínims de seguretat que evitin els riscos d'indisponiblitat dels Fitxers que poguessin produir-se com a conseqüència d'incidències fortuïtes o intencionades.
L'accés als locals on es trobin els Fitxers haurà d'estar restringit exclusivament a les persones Administradores de Sistemes i de Bases de Dades que han de realitzar tasques de manteniment per a les que sigui imprescindible l'accés físic.
L' accés a la sala de servidors estarà restringit al personal de la Secció de Sistemes d'Informació, al personal acreditat per la Presidència de la Comissió de Seguretat i al personal dels serveis de neteja.
El personal de la Secció de Sistemes d'Informació, per tal de poder realitzar els torns de guàrdia així com les corresponents actuacions de manteniment, disposarà d'una clau per poder accedir a les instal·lacions les 24 hores dels 7 dies de la setmana i es responsabilitzarà del seu tancament en el moment d'abandonar el local i de no permetre l'accés a persones no autoritzades.
La resta d'instal·lacions municipals, un cop finalitzi el servei de vigilància permanent, romandran tancades amb clau i protegides amb un sistema d'alarma. La sol·licitud d'accés fora de l'horari laboral es farà a través del formulari estàndard que s'elabori per la Comissió de Seguretat.
Quan sigui necessari l'accés als locals de personal extern sempre ho farà acompanyat de personal autoritzat i es registrarà posteriorment en l'aplicació de control d'accessos. Aquest registre en conservarà durant el període de temps que

acordi la Comissió de Seguretat que, a aquests efectes, elaborarà la *Taula de conservació de la documentació*.
Semestralment, el personal de la Secció de Sistemes d'Informació procedirà a relacionar el Registre d'accessos a la sala de servidors des de l'aplicació de control de presència i emetrà un informe d'incidències[7] i, un cop aplicades les mesures pertinents, efectuarà el corresponent arxiu durant d'interval de temps indicat a la *Taula de conservació de la documentació*.

Article 20. **Dispositius d'emmagatzematge dels fitxers no automatitzats**

Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin la seva obertura.
Quan les característiques físiques no permetin adoptar la mesura descrita a l'apartat anterior, la Comissió de Seguretat adoptarà les mesures alternatives que impossibilitin l'accés a persones no autoritzades.
Els armaris, els arxivadors o altres elements en els quals s'emmagatzemin fitxers no automatitzats que continguin dades personals de nivell alt s'hauran d'ubicar en àrees amb accés protegit amb portes dotades de sistemes d'obertura amb clau o altre dispositiu equivalent. Aquestes àrees hauran de romandre tancades quan no sigui necessari l'accés als documents inclosos als fitxers.
Quan, ateses les característiques dels locals, no fos possible complir allò establert a l'apartat anterior, la Comissió de Seguretat adoptarà mesures alternatives que garanteixin el mateix nivell de seguretat.

Article 21. **Controls de Seguretat als llocs de treball**

Sense perjudici de les instruccions que pugui dictar l'alcaldia, a proposta de la Comissió de Seguretat, caldrà garantir, com a mínim, l'acompliment de les normes que es detallen a continuació:

a) Tots els armaris i els calaixos que continguin documents amb dades de caràcter personal o confidencial hauran de tancar-se amb clau en finalitzar la jornada laboral.
b) Els enviaments d'informació de caràcter personal o confidencial entre les diferents unitats administratives s'haurà de fer mitjançant l'ús de missatgeria interna o sota condicions de confidencialitat amb la utilització de carpetes o sobres adientment tancats.
c) Cada lloc de treball estarà sota la responsabilitat de la persona que l'ocupi, que haurà de garantir que la informació de què disposa no pugui ser visualitzada per persones no autoritzades.

[7] S'hi incorpora, com a ANNEX 7, el document que conté el model de l'*Informe del registre dels accessos a l'aplicació de control d'accessos al CPD* (codi PDPL02).

d) Les pantalles, les impressores o altre tipus de dispositius connectats al lloc de treball hauran d'estar físicament ubicats en llocs que permetin garantir aquesta confidencialitat.
e) Quan la persona responsable d'un lloc de treball l'abandoni, ja sigui temporalment o en finalitzar el seu torn de treball, l'haurà de deixar en un estat que impedeixi la visualització de les dades protegides.
f) En la utilització dels faxos i impressores, locals i compartides, es garantirà que no quedin documents amb dades personals impresos a la safata de sortida, que hauran d'ésser retirats, immediatament, una vegada impresos.
g) En els enviaments a través de fax s'utilitzarà la plantilla model que elaborarà la Comissió de Seguretat.
h) Tota la informació i documentació desenvolupada en l'àmbit laboral és de propietat exclusiva de l'Ajuntament de Cerdanyola del Vallès i, en conseqüència, no se'n podrà fer un ús privat ni treure'n un benefici personal.
i) L'ús dels recursos que l'Ajuntament de Cerdanyola del Vallès posa a disposició del lloc de treball únicament podrà tenir una finalitat professional. No s'autoritza l'ús personal d'aquests recursos.
j) Tots els ordinadors que no tinguin una persona assignada i que no s'utilitzin seran retirats prèvia comunicació per part de la persona encarregada del tractament a la Secció de Sistemes d'Informació.
k) Els canvis en la ubicació física d'equips han de ser executats per personal tècnic, per la qual cosa cal preveure'ls i demanar-los amb temps d'antelació suficient mitjançant la corresponent petició a través de l'aplicació de gestió d'incidències.
l) Els llocs de treball des dels quals es té accés als sistemes d'informació tindran una configuració fixa en les seves aplicacions i sistemes operatius que només podrà ser canviada sota l'autorització de la Presidència de la Comissió de Seguretat o per Administradors de Sistemes i de Bases de Dades autoritzats.
m) Els llocs treball podran tenir deshabilitats els mecanismes que permeten el registre de les operacions realitzades o eliminar els arxius que es generen per a tal finalitat de manera manual.
n) Per tal de garantir un adequat funcionament del sistema informàtic és obligatori atendre els missatges i/o avisos dels Responsables de sistemes i executar les accions que s'hi indiquin.
o) Els equips informàtics s'hauran de deixar en el millor estat de disponibilitat, ordre i neteja.
p) Els equips s'hauran d'apagar cada dia abans d'abandonar el lloc de treball per tal d'estalviar energia i permetre les tasques de manteniment dels equips i de les aplicacions.
q) Totes les persones usuàries que disposin d'ordinador portàtil hauran d'assegurar-se que estan protegits per contrasenya.
r) Serà responsabilitat de les persones usuàries d'ordinadors portàtils habilitar les mesures físiques de seguretat que assegurin la protecció, dels equips i de les

dades que contenen. Els equips no es deixaran a l'interior de vehicles aparcats en llocs on tothom pugui veure'ls ni s'exposaran a la calor i a camps magnètics.

s) No es discutiran assumptes confidencials per telèfon ni per telèfon mòbil en ubicacions que no permetin garantir-ne la confidencialitat.

Article 22. **Inventari dels equips assignats als llocs de treball**

Tots els equips informàtics (ordinadors, impressores, faxos, unitats externes i altres perifèrics) assignats als llocs de treball hauran d'estar degudament inventariats a l'aplicació informàtica d'Inventari d'Elements.

Els equips que hagin de ser reassignats a un nou lloc de treball hauran de ser degudament formatats i reconfigurats abans d'una nova assignació.

CAPÍTOL II. CONTROL D'ACCESSOS ALS RECURSOS DEL SISTEMA

Article 23. **Accés al sistema**

L'accés al sistema informàtic estarà restringit al personal autoritzat. Prèviament a l'accés al sistema es visualitzarà un missatge d'inici de sessió[8].

L'horari d'accés a les dependències coincidirà amb el corresponent a la jornada habitual del treballador; no obstant això, si cal accedir en un horari més ampli per realitzar funcions assignades al lloc de treball, caldrà sol·licitar-ho expressament i requerirà conformitat de la persona encarregada del tractament. Les peticions es conservaran, durant d'interval de temps indicat a *la Taula de conservació de la documentació* que elabori la Comissió de Seguretat.

Si l'aplicació informàtica que permet l'accés als Fitxers no compta amb un control d'accés, serà el sistema operatiu on s'executa aquesta aplicació el que impedeixi l'accés no autoritzat mitjançant el control dels codis d'usuari i contrasenyes que s'especifiquen als articles 27 i 28 d'aquest Reglament.

En qualsevol cas, es controlaran els intents d'accés fraudulent als Fitxers i es limitarà el nombre màxim d'intents fallits i, quan sigui tècnicament possible, es guardaran, en un fitxer auxiliar, la data, l'hora, el codi i la clau erronis que s'han introduït, així com altres dades rellevants que ajudin a descobrir l'autoria d'aquests intents d'accés fraudulents.

Article 24. **Accés a la documentació**

L'accés als fitxers no automatitzats es limitarà exclusivament al personal autoritzat que precisi d'aquests recursos per al desenvolupament de les seves funcions, els quals hauran d'estar autoritzats per la persona encarregada del tractament.

[8] S'hi incorpora, com a ANNEX 8, el *Missatge d'inici de sessió* (codi PDPL24).

S'establiran mecanismes que permetin identificar el personal que accedeix a la documentació dels fitxers no automatitzats.
Els fitxers no automatitzats seran objecte d'aplicació de les mesures de seguretat que el RLOPD estableix per aquesta tipologia de fitxers en funció del seu nivell de dades[9].

Article 25. **Entorn de Sistema Operatiu i de Comunicacions**
El mètode establert per accedir a les dades protegides dels Fitxers és el sistema informàtic la descripció del qual s'incorpora en annex[10] i s'haurà regular l'ús i accés de les parts del sistema operatiu, eines o programes d'utilitat, o de l'entorn de comunicacions, de forma que s'impedeixi l'accés no autoritzat a les dades dels Fitxers.
El sistema operatiu i de comunicacions dels Fitxers haurà de tenir al menys una persona responsable que, com a Administradora de Sistemes i de Bases de Dades, haurà d'estar relacionada a les bases de dades de l'Ajuntament com a personal autoritzat per accedir als Fitxers.
En cas que els Fitxers es trobin ubicats en un ordinador personal i sigui accessible únicament mitjançant una aplicació local monousuària, l'Administrador de Sistemes i de Bases de Dades podrà ser la mateixa persona usuària que accedeix habitualment als Fitxers.
Cap eina o programa d'utilitat haurà de permetre l'accés als Fitxers per mitjans en brut, és a dir, no elaborats o editats, a les dades dels Fitxers, com les anomenades *queries*, editors universals, analitzadors de fitxers, etc., que hauran d'estar sota el control de les persones Administradores de Sistemes i de Bases de Dades autoritzades.
Si l'aplicació o sistema d'accés als Fitxers utilitzés usualment fitxers temporals, fitxers de *log* o qualsevol altre medi en què poguessin ser enregistrades còpies de les dades protegides, les persones Administradores de Sistemes i de Bases de Dades garantiran que aquestes dades no són accessibles posteriorment per personal no autoritzat.

Article 26. **Accés a unitats de disc**
Cada persona usuària del sistema disposarà d'un espai d'accés i ús reservat en el disc del Servidor Corporatiu, per tal d'emmagatzemar aquella informació que cap altra persona usuària estigui autoritzada a accedir.

---

[9] S'hi incorpora, com a ANNEX 9, el document que conté les mesures de seguretat per als fitxers no automatitzats, identificat com a *Tractaments no automatitzats de dades* (codi PDIN02)

[10] S'hi ha incorporat, com a ANNEX 5, el document que conté la descripció del sistema operatiu, identificat com a *Descripció del sistema informàtic d'accés als Fitxers* (codi PDPL10).

L'espai reservat de disc del Servidor Corporatiu no es podrà utilitzar per instal·lar o copiar programari o programes executables, llevat de les autoritzacions expresses que realitzi la presidència del la Comissió de Seguretat. En cap cas, s'hi podrà instal·lar informació no relacionada amb les tasques pròpies del lloc de treball.
Sense perjudici d'allò que es determina en l'article següent, cada persona usuària podrà tenir accés a l'espai de disc reservat per a la unitat administrativa en què estigui enquadrat. En aquest àmbit podrà compartir fitxers o documents emmagatzemats amb els mateixos privilegis i responsabilitats que la resta de persones usuàries amb accés al disc.
El disc corresponent a l'ordinador personal no es podrà utilitzar per emmagatzemar informació de dades afectades per la LOPD i es destinarà únicament a la instal·lació del programari necessari en l'àmbit de les funcions atribuïdes al lloc de treball. La responsabilitat per la pèrdua d'informació del disc dur s'atribueix a la persona usuària.
Les persones usuàries dels ordinadors connectats a la xarxa local que requereixin extreure informació per necessitats del lloc de treball fora de l'Ajuntament, en qualsevol de les seves formes (en suports físics o lògics), hauran d'ajustar les seves actuacions a allò que s'estableix en aquest Reglament, especialment pel que fa a la gestió general i a la reutilització de suports.

Article 27. **Assignació de claus d'identificació**

Les persones Administradores de Sistemes i de Bases de Dades assignaran una clau d'identificació individualitzada a cada persona usuària, amb un nom d'accés i una contrasenya.
En el moment de procedir a l'assignació de la paraula de pas, caldrà atendre les pautes següents:

a) Evitar que contingui paraules convencionals que puguin existir en un diccionari. Tampoc escollir aquelles que resultin d'escriure-les del revés, noms propis, sobrenoms o paraules en idioma estranger.
b) Evitar escriure números de telèfon, adreces, anys o dates completes de naixement.
c) Utilitzar claus amb la major longitud possible. Es recomana un mínim de sis caràcters.
d) La nova paraula de pas assignada no podrà ser igual a les quatre anteriors.
e) Evitar seqüències de números (*567890*), d'alfabet (*hijklm*) o de teclat (*qwerty*).

Les contrasenyes es canviaran mitjançant el mecanisme i periodicitat que es determini per la Comissió de Seguretat[11], d'acord amb les prevencions establertes en aquest Reglament.

[11] S'hi ha incorporat, com a ANNEX 6, el document dels *Procediments de control d'accessos, suport, recuperació i gestió* (codi PDPL14).

Les persones encarregades del tractament, en el moment de demanar els accessos del personal al seu càrrec a través de l'aplicació de gestió d'incidències, garantiran que aquestes únicament tinguin accés a aquelles dades i recursos que precisin per al desenvolupament de les seves funcions.
L'assignació de les claus d'identificació es farà mitjançant l'enviament al lloc on s'indiqui per part de la Presidència de la Comissió de Seguretat, per part de la persona encarregada del tractament, del formulari[12] d'alta de persona usuària a la xarxa informàtica, degudament emplenat. Caldrà indicar-hi els recursos del sistema que s'han de posar a disposició de la persona usuària (unitats de disc compartides, programari ofimàtic, aplicacions corporatives a les que tindrà accés, perfil, etc.) i si la clau és temporal o definitiva. També s'hi especificarà si la persona usuària ha de tenir accés a internet, en funció de les necessitats del lloc de treball.
La modificació dels privilegis d'accés assignats a cada persona usuària es tramitarà de la mateixa manera que l'assignació inicial.
L'arxiu on s'emmagatzemin les contrasenyes haurà d'estar protegit i sota la responsabilitat de les persones Administradores de Sistemes i de Bases de Dades.

Article 28. **Clau d'identificació individualitzada**
La clau d'identificació serà personal, confidencial i intransferible, i no es podrà compartir amb altres persones usuàries.
Correspondrà a la persona usuària titular de la clau d'identificació individualitzada la responsabilitat associada a totes aquelles accions i transaccions que s'enregistrin en els Fitxers d'Auditoria sota el compte que li hagi estat assignat.

CAPÍTOL III. CONTRASENYES

Article 29. **Confidencialitat de les contrasenyes**
La contrasenya d'accés al sistema i/o aplicacions específiques i la de desbloqueig del protector de pantalla són absolutament confidencials.
És responsabilitat de cada persona usuària garantir un ús correcte d'aquestes claus. No es podran anotar en llocs visibles o accessibles a persones no autoritzades.

En finalitzar la jornada laboral, o en el supòsit d'absència del lloc de treball, la persona usuària haurà de prendre les mesures oportunes per evitar que el seu accés al sistema pugui ser reemplaçat per terceres persones.

[12] S'hi incorpora, com ANNEX 10, el document que conté el *Formulari d'alta de persona usuària a la xarxa informàtica* (codi PDPL23).

Quan una persona usuària tingui coneixement o consideri probable que s'han realitzat accions de consulta, utilització, manipulació, modificació, destrucció o transmissió dels recursos protegits per aquest Reglament a través de la seva clau d'accés al sistema, ho posarà immediatament en coneixement de les persones Administradores de Sistemes i de Bases de Dades mitjançant l'aplicació de gestió d'incidències, i es procedirà, de forma immediata, a modificar la seva contrasenya i a iniciar les diligències necessàries per determinar l'abast de les accions i les persones responsables.

Article 30. **Periodicitat de canvi de contrasenyes**

La contrasenya d'accés al sistema o a les aplicacions d'ús concret, podrà ser canviada per la persona usuària en qualsevol moment.

En tot cas, el sistema informàtic garantirà que les contrasenyes no pugin tenir una vigència superior als tres mesos.

El canvi de contrasenya serà realitzat bé directament per la persona usuària o per les persones Administradores de Sistemes i de Bases de Dades quan motius tècnics o de configuració de l'aplicació impossibilitin l'actuació de la usuària.

CAPÍTOL IV. MECANISMES D'AUTORITZACIÓ I ACCÉS A LES DADES

Article 31. **Mecanismes de seguretat d'accés**

Les aplicacions corporatives disposaran de mecanismes de seguretat d'accés basats en el disseny de rols o perfils de persones usuàries, en funció dels quals es distingiran les operacions permeses a realitzar.

L'assignació del rol i de l'accés adequat de cada persona usuària s'ajustarà a allò que determina l'article 27 d'aquest Reglament.

Article 32. **Altes, baixes i suspensió d'accessos a les persones usuàries**

La persona encarregada del tractament en l'àmbit de treball de cada persona usuària comunicarà immediatament a les persones Administradores de Sistemes i de Bases de Dades, de conformitat amb les instruccions establertes, a través de l'aplicació de gestió d'incidències, les altes, les baixes, les suspensions i/o els canvis d'ubicació que puguin tenir incidència sobre els accessos de les persones usuàries.

Rebuda la comunicació indicada en l'apartat anterior, les persones Administradores de Sistemes i de Bases de Dades procediran a modificar les autoritzacions o bloquejar l'accés de les persones usuàries. Igualment, les Administradores de Sistemes i de Bases de Dades bloquejaran els accessos de les persones usuàries que no realitzin moviments d'accés per un període superior a 40 dies; els quals podran ser restablerts amb el mateix procediment que per a l'assignació inicial de rol i d'accés.

CAPÍTOL V. ACCESSOS AL SISTEMA

Article 33. **El Registre de Seguretat del Sistema**

S'elaborarà un Registre de Seguretat del Sistema que constarà d'una relació exhaustiva amb la identificació de totes les persones usuàries amb accés al sistema i dels recursos físics i lògics als quals tinguin accés.

Es procedirà a registrar, per a cada aplicació, els diferents perfils o rols amb els seus respectius privilegis, amb detall de l'assignació d'usuària per rol en funció de les responsabilitats de gestió de dades que li hagin estat assignades al lloc de treball corresponent.

Les sol·licituds que es produeixin en relació als accessos, al sistema o a aplicacions departamentals o corporatives es faran mitjançant l'aplicació informàtica corresponent, on quedaran anotades.

Article 34. **Registre d'accessos**

Les connexions de les persones usuàries als sistemes corporatius de nivell mitjà i alt seran mantingudes i registrades mitjançant el procediment d'*accounting.*

Amb la periodicitat que determini la Comissió de Seguretat, que no serà superior a sis mesos, es procedirà a realitzar el resum de l'activitat del període i elaborar un informe d'accés al sistema, que es conservarà durant el termini de temps que s'estableixi per la Comissió de Seguretat per a la conservació de la documentació.

Els intents d'accés erronis i reiterats, registrats al fitxer de *log*, seran analitzats setmanalment per les persones Administradores de Sistemes i de Bases de Dades per determinar l'existència d'incidències de maquinari o programari o, pel contrari, si es tracta d'accessos no autoritzats. En aquest darrer cas, es prendran les mesures oportunes de seguiment de les incidències.

Els mecanismes que permeten el registre d'accessos estaran sota el control directe de la Presidència de la Comissió de Seguretat.

No es desactivaran, en cap cas, els mecanismes que permeten el registre d'accessos al sistema.

La Presidència de la Comissió de Seguretat s'encarregarà de revisar, al menys un cop al mes, la informació de control registrada i elaborarà un informe de les revisions realitzades i els problemes detectats, que elevarà a la Comissió de Seguretat.

CAPÍTOL VI. ÚS DE PROGRAMARI ESPECÍFIC O DE PROPÒSIT GENERAL

Article 35. **Productes de programari**

Els productes de programari destinats al tractament automatitzat de dades personals hauran d'incloure a la seva descripció tècnica el nivell de seguretat, bàsic, mitjà o alt, que permetin assolir. Aquesta informació s'afegirà a l'inventari del programari[13].

Article 36. **Instal·lació de programari**

L'ús de les aplicacions corporatives per part de les persones usuàries se sol·licitarà per la persona encarregada del tractament, de conformitat amb l'article 27 d'aquest Reglament.

Només s'hi podran instal·lar programaris o programes respecte dels quals es disposi de la corresponent llicència d'ús.

Les instal·lacions de programaris o programes només s'efectuaran per les persones de Sistemes d'Informació, que no les realitzaran si resulten incompatible amb la resta del sistema.

En cap cas, les persones usuàries poden instal·lar programaris o programes en el sistema corporatiu.

Article 37. **Descàrrega de programari des d'Internet**

Les persones usuàries no podran descarregar d'internet, ni instal·lar, cap tipus de programari, fins i tot els programaris de prova o els gratuïts i similars.

Si es cal fer una instal·lació d'aquest tipus de programes, se sol·licitarà, a través de l'aplicació de gestió d'incidències, per la persona encarregada del tractament, a les persones Administradores de Sistemes i de Bases de Dades, que verificaran el programari i procediran, si resulta procedent, a la seva instal·lació.

La data d'instal·lació del programari, les seves característiques i les condicions d'ús i es registrarà en la fitxa de l'equip.

Article 38. **Verificació del programari instal·lat**

En execució del Pla d'Auditoria interna, el personal de la Secció de Sistemes d'Informació verificarà que en cada ordinador personal només estigui instal·lat el programari autoritzat i procedirà a l'eliminació d'aquells programes que no constin en la fitxa de registre de programari; sense perjudici de les responsabilitats que s'hi pugui exigir a les persones autores de la instal·lació de programari no autoritzat.

[13] S'hi incorpora, com a ANNEX 11, el document que conté l'*Inventari del programari («software»)* (PDPL04).

CAPÍTOL VII. ACCÉS A INTERNET

Article 39. **Sistema de Firewall**

La connexió de la xarxa local amb l'exterior, als efectes de protecció del Sistema d'Informació Municipal, es realitzarà únicament a través del sistema *firewall* o tallafocs.

Els recursos d'accés públic a la xarxa estaran ubicats en la zona exterior del *firewall*.

Article 40. **Accés a Internet i correu electrònic**

La sol·licitud per part de les persones usuàries d'accés a Internet es realitzarà de conformitat amb el procediment que es detalla en l'article 27 d'aquest Reglament.

Tots els comptes d'accés a Internet i els de correu electrònic seran personalitzats per a cada persona usuària, que en serà responsable del bon ús d'ambdós serveis.

En cap cas es podran modificar les configuracions dels navegadors de l'equip, ni l'activació de servidors o ports sense autorització de la Presidència de la Comissió de Seguretat o de les persones Administradores de Sistemes i de Bases de Dades.

Les persones usuàries i les persones Administradores de Sistemes i de Bases de Dades esborraran periòdicament totes les dades de directoris temporals (*Temp i Caché*).

L'Ajuntament de Cerdanyola del Vallès posa a disposició del personal al seu servei un compte de correu per a les comunicacions internes i externes que hagin de dur a terme, sempre que aquestes estiguin relacionades amb les funcions pròpies del seu lloc de treball i que, per tant, es destinin a un ús estrictament laboral.

Excepcionalment, s'autoritza l'ús responsable del correu electrònic per a usos personals, amb garantia de la seva privacitat, sempre que:

a) No suposi una dedicació important de temps o interfereixi en el rendiment del lloc de treball.
b) No suposi un alt cost per a l'Ajuntament.
c) No es tracti d'enviaments massius, de missatges en cadena o de tipus piramidal.
d) No s'utilitzi per al lucre personal.

De la mateixa manera, es determina que queda expressament prohibit enviar missatges de correu electrònic quan aquests:

a) Infringeixin les normes del Copyright o de la propietat intel·lectual.
b) Atemptin contra els drets de terceres persones o del propi Ajuntament.
c) Siguin difamatoris, fraudulents, obscens, amenaçadors o incorrin en conductes il·legals o il·lícites.
d) Falsifiquin les capçaleres del correu.
e) Trametin continguts expressament prohibits en aquest Reglament.
f) Recullin correus de bústies d'altres proveïdors d'Internet.
g) Pretenguin enviar correu propi mitjançant comptes aliens sense consentiment del seu titular.

h) Vulguin efectuar-se atacs, amb objecte d'impossibilitar o obstruir sistemes informàtics, dirigits a una persona usuària o al propi sistema de correu, així com l'enviament d'un nombre elevat de missatges per segon, o qualsevol variant, que tingui per objecte la paralització del servei per saturació de les línies, de la capacitat de CPU del servidor, de l'espai en disc de servidors o terminals o qualsevol altra pràctica similar.

i) Vulguin enviar-se missatges que comprometin la reputació de l'Ajuntament a fòrums de discussió, llistes de distribució o grups de noticies.

j) S'incorri en alguna de les situacions indicades a l'apartat anterior.

L'Ajuntament es reserva el dret a controlar els missatges de correu electrònic quan hi hagi indicis que s'ha vulnerat la política d'utilització del correu electrònic descrita en aquest Reglament o per causa d'alguna obligació legal.

No es farà un ús dels serveis de xat, fòrums o llocs similars més enllà de les funcions que es derivin del desenvolupament del lloc de treball. L'accés a pàgines de jocs o qualsevol altre tipus d'aplicació d'oci d'ús no justificat es considerarà com a ús inadequat dels recursos proveïts per l'Ajuntament.

Per tal de garantir la integritat de la informació emmagatzemada en els servidors corporatius i el bon ús que s'hi fa d'Internet, les persones Administradores de Sistemes i de Bases de Dades analitzaran mensualment els llocs d'Internet als quals s'accedeix des de la xarxa corporativa.

Amb la finalitat d'evitar possibles infeccions de l'ordinador, no s'obriran els arxius adjunts a correus electrònics que provinguin de remitents desconeguts o no segurs.

D'acord amb el procediment que s'estableixi per part de la Comissió de Seguretat, en el moment en què es produeixi una baixa laboral, la unitat de Sistemes d'Informació redireccionarà, durant el període de temps que s'estableixi, que no serà inferior a un mes, els comptes de correu electrònic a d'altres actius, autoritzats per la persona que causa baixa mitjançant la sol·licitud corresponent. Passat aquest termini, l'Ajuntament té la facultat d'accedir al compte de correu electrònic de la persona que hagi causat baixa de l'Ajuntament i de reassignar els nous correus a l'adreça de la persona que desenvolupi les funcions que anteriorment corresponien a la persona que ha causat baixa[14].

Les persones usuàries són responsables de totes les activitats realitzades amb els comptes d'accés i la seva corresponent bústia de correu proveïts per l'Ajuntament.

Les persones usuàries no permetran la utilització del compte i/o la corresponent bústia a persones no autoritzades.

Les persones usuàries han de ser conscients dels riscos que suposa l'ús indegut de les adreces de correu electrònic subministrades per l'Ajuntament i respondran per la seva conducta, de conformitat amb aquest Reglament.

[14] S'hi ha incorporat, com ANNEX 10, el document que conté el *Formulari d'alta de persona usuària a la xarxa informàtica* (PDPL23).

No es podran enviar correus de contingut personal a persones que hagin manifestat que no en volen rebre. L'Ajuntament de Cerdanyola del Vallès, a través de la unitat d'Organització i Recursos Humans, rebrà les reclamacions en aquest sentit i adoptarà les mesures que consideri convenients per evitar aquestes conductes, que podran ser sancionades.
Sense perjudici d'allò que estableixi el conveni col·lectiu i l'Acord sobre condicions laborals del personal funcionari de l'Ajuntament de Cerdanyola del Vallès, els/les representants dels treballadors i de les treballadores i la representació dels sindicats podran fer ús del correu electrònic per difondre informació estrictament relacionada amb la seva activitat sindical o de representació social. No obstant això, el personal al servei de l'Ajuntament de Cerdanyola del Vallès té dret a mostrar la seva oposició i que s'impedeixi la recepció de missatges amb contingut sindical en el seu correu electrònic corporatiu, llevat que es tracte d'un període electoral, en què prevaldrà, en tot cas, el dret a l'activitat sindical.

Article 41. **Entrada i sortida de dades per xarxa**

Caldrà aplicar les mesures que impedeixin l'accés per part de terceres persones no autoritzades a totes les entrades i les sortides de dades de fitxers amb dades de caràcter personal de nivell alt que s'efectuïn mitjançant correu electrònic.
D'acord amb les instruccions i el procediment que determini la Comissió de Seguretat, es guardaran còpies de tots els correus que involucrin entrades o sortides de dades d'aquests tipus de fitxers en directoris protegits i sota el control de la persona que es designi com a responsable. Es mantindran còpies d'aquests correus durant almenys dos anys. També es guardarà, durant un mínim de dos anys i en directoris protegits, una còpia dels fitxers rebuts o transmesos per sistemes de transferència de fitxers per xarxa, juntament amb un registre de la data i hora en què es va realitzar l'operació i el destí dels fitxers enviats.
Quan les dades dels Fitxers siguin enviades a través de xarxes públiques o xarxes sense fils de comunicacions electròniques es realitzarà mitjançant l'encriptació de les dades o utilitzant qualsevol altre mecanisme de manera que aquestes només puguin ser llegides i interpretades pel destinatari.
La unitat de Sistemes d'Informació garantirà que, en tot moment, el servidor del correu electrònic corporatiu afegeixi a tots els correus externs una nota d'avís legal sobre la confidencialitat de les dades personals que s'hi continguin.
Serà responsabilitat de les persones encarregades del tractament l'obtenció del consentiment a què es refereix l'article 21 de la *Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del comercio electrónico,* sempre que s'efectuïn trameses electròniques amb caire de difusió i/o d'informació general.

Article 42. **Utilització de sistemes antivirus**

Tots els equips que disposin de programari d'accés a Internet hauran de tenir instal·lat i activat, en tot moment, el programari antivirus. Les configuracions de protecció instal·lades de forma estàndard no podran ser modificades per les

persones usuàries. És competència exclusiva del personal de Sistemes d'Informació, l'actualització periòdica de les noves versions antivirus.

Article 43. **Infecció d'ordinadors**

Si una persona usuària té la certesa o sospita d'una possible infecció de l'ordinador, avisarà immediatament la unitat de Sistemes d'Informació per tal que sigui el personal adscrit a aquesta qui avaluï l'origen d'aquesta infecció i les conseqüències que se'n poden derivar. Caldrà anotar el text literal de tots els missatges que enviï el sistema per tal de posar-los en coneixement del personal de Sistemes d'Informació.

Si el personal de Sistemes d'Informació no pot actuar-hi immediatament, l'ordinador serà etiquetat com a «INFECTAT» i no es podrà utilitzar fins que s'hagi resolt la infecció per part del personal de Sistemes d'Informació.

Si es coneix la procedència del virus, el personal de Sistemes d'Informació informaran a la persona o entitat emissora sobre la seva existència.

TÍTOL IV. INTERCANVIS D'INFORMACIÓ I TRASPASSOS DE FITXERS ENTRE PERSONES USUÀRIES DEL SISTEMA (TRÀNSITS D'INFORMACIÓ I FITXERS)

CAPÍTOL I. INTERCANVI DE FITXERS AMB PERSONES USUÀRIES DEL SISTEMA QUE NO PERTANYEN AL MATEIX GRUP FUNCIONAL QUE LA PERSONA EMISSORA

Article 44. **Intercanvi intern d'informació**

L'intercanvi dels fitxers aïllats es realitzarà, preferentment, mitjançant els recursos compartits dels servidors de fitxers destinats a aquesta finalitat.

CAPÍTOL II. INTERCANVI DE FITXERS AMB PERSONES I ENTITATS ALIENES AL SISTEMA

Article 45. **Intercanvis d'informació amb persones i entitats externes a l'Ajuntament**

Els intercanvis d'informació amb persones, organitzacions, organismes públics o institucions externes a l'Ajuntament estaran subjectes a la normativa de règim local aplicable en cada moment així com a les restriccions i supòsits i procediments establerts[15].

La Comissió de Seguretat serà l'encarregada d'elaborar i actualitzar i garantir-ne el coneixement general dels criteris a seguir quan l'intercanvi d'informació impliqui dades del padró municipal d'habitants. Les persones usuàries seguiran estrictament els criteris establerts[16].

Igualment, la Comissió de Seguretat elaborarà, actualitzarà i garantirà el coneixement general dels criteris de protecció de dades de caràcter personal en el cas de publicacions de dades de persones que concorrin en processos selectius i en tots aquells supòsits en què resulti convenient establir-ne criteris específics.

CAPÍTOL III. EXTRACCIÓ I INTRODUCCIÓ D'INFORMACIÓ EN EL SISTEMA

Article 46. **Extracció d'informació del Sistema**

L'extracció d'informació de caràcter personal referent a persones alienes a la Corporació que estigui emmagatzemada en el sistema, en qualsevol tipus de suport, físic, magnètic o òptic, haurà de ser sol·licitada i autoritzada per les persones encarregades del tractament mitjançant l'aplicació informàtica corresponent i la informació referent a la cessió de les dades es conservarà durant el període de temps establert.

Per als suports que continguin dades de caràcter personal de nivell mitjà i alt, la transacció efectuada serà anotada al Registre corresponent. Igualment, si es tracta de cessió de dades en suport paper, caldrà conservar –ne la còpia durant el termini establert.

---

[15] S'hi incorpora, com a ANNEX 12, el document que conté el *Procediment de captació de dades* (PDPR05).

[16] S'hi incorpora, com a ANNEX 13, el document que conté les *Instruccions sobre la cessió de dades del padró municipal d'habitants* (PDIN05).

És responsabilitat de la persona usuària garantir l'exactitud del contingut dels fitxers extrets, així com el compliment de les normes que, per a l'intercanvi d'informació i sortida de dades fora de l'Ajuntament, s'estableixen en aquest Reglament, especialment als capítols I i II d'aquest títol i a l'article 49.

Article 47. **Introducció d'informació en el Sistema**

La incorporació d'informació des d'un suport extern seguirà el mateix procediment indicat a l'article anterior i s'indicarà en el Registre corresponent.

El contingut del suport serà objecte del test antivirus, que abastarà tots els fitxers, amb inclusió dels fitxers que estiguessin comprimits. El personal de Sistemes d'Informació garantirà l'acompliment d'aquesta norma.

Article 48. **Fitxers temporals**

Tots els fitxers temporals hauran de complir el nivell de seguretat que li correspongui segons els criteris establerts en els articles 80 i 81 del *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* i hauran de constar inscrits en l'inventari de fitxers corporatius i temporals. i guardar-se en unitats de xarxa, de conformitat amb l'article 26 d'aquest Reglament.

Els fitxers temporals seran esborrats en el moment en què hagin deixat de ser necessaris per a la finalitat per a la qual es van crear i, una vegada esborrats, seran eliminats de l'inventari de fitxers corporatius i temporals. S'excepciona els casos en què calgui conservar els fitxers temporals per motius històrics, estadístics o científics. Correspon a la presidència de la Comissió de Seguretat garantir el compliment d'aquesta norma.

En els fitxers generats amb la finalitat de crear impresos basats en una plantilla estàndard no s'enregistraran dades de caràcter personal.

En els camps d'observacions dels fitxers o documents no es permet incloure-hi qüestions relatives a la vida privada i/o l'honorabilitat de les persones, especialment si fa referència a dades considerades sensibles (raça, religió, creences, vida sexual, salut, afiliació sindical o política, etc.) o que puguin resultar despectives per a la persona.

Els documents seran protegits mitjançant contrasenya per part de les persones responsables del seu tractament.

TÍTOL V. GESTIÓ DE SUPORTS D'EMMAGATZEMATGE D'INFORMACIÓ

Article 49. **Gestió general de suports**

Les persones Administradores de Sistemes i de Bases de Dades mantindran actualitzat el Registre on hi constin les circumstàncies relatives a l'entrada i sortida de suports magnètics o òptics que continguin informació subjecta a protecció legal, de conformitat amb allò que s'estableix a l'apartat quart d'aquest article.

Els suports que continguin dades dels fitxers, bé com a conseqüència d'operacions intermèdies pròpies de l'aplicació que els tracta o bé com a conseqüència de processos periòdics de recolzament o qualsevol altra operació esporàdica, haurien de:

1. Estar clarament identificats amb una etiqueta externa que indiqui de quins fitxers es tracta, quin tipus de dades conté, procés que les ha originat i data de creació.
2. Estar inventariats degudament a l'aplicació informàtica en què s'enumeren els suports generats. Aquest Registre s'haurà de conservar durant el temps establert.

Quan, per les característiques físiques del suport, sigui impossible el compliment de les obligacions indicades a l'apartat anterior, la Presidència de la Comissió de Seguretat haurà de deixar constància motivada per escrit d'aquest fet.

La identificació dels suports que continguin dades de caràcter personal que es considerin especialment sensibles es podrà realitzar amb utilització de sistemes d'etiquetatge comprensibles i amb significat que permetin, a les persones usuàries amb accés autoritzat als suports i documents, identificar el seu contingut, i que dificultin la identificació per a la resta de persones

Els suports que continguin dades dels sistemes informàtics hauran de ser emmagatzemats en llocs als quals no tinguin accés persones que no estiguin incloses en les aplicacions informàtiques que enumeren les persones autoritzades per accedir als fitxers.

La Presidència de la Comissió de Seguretat mantindrà un Registre d'Entrades i Sortides i guardarà els albarans que lliura l'empresa encarregada de la custòdia de les còpies de seguretat.

Les entrades i sortides de suports que continguin dades personals es registraran a cadascun de les unitats i hauran de ser autoritzades per la persona encarregada del tractament. En qualsevol cas s'haurà d'indicar:

a) Tipus de suport.
b) Data i hora.
c) Emissora/Destinatària.
d) Nombre de suports o documents.
e) Tipus d'informació que contenen.
f) Forma d'enviament.

g) Destinatari o persona responsable de la recepció/lliurament degudament autoritzades.

Quan els suports amb dades personals hagin de sortir fora dels locals en què es trobin ubicats els fitxers, s'adoptaran les mesures necessàries per impedir qualsevol subtracció, pèrdua o accés indegut a la informació durant el transport.

La sortida fora dels locals on estan ubicats els Fitxers de suports, informàtics i físics, que continguin dades dels fitxers, inclosos els adjunts al correus electrònics, haurà d'estar expressament autoritzada per la persona Responsable dels Fitxers. En aquests casos, caldrà utilitzar el Registre d'Entrades i Sortides de suports, el qual s'haurà de conservar durant els temps establert.

No es tractaran dades personals de nivell alt en dispositius portàtils que no permetin el seu xifrat. No obstant això, en el supòsit que sigui estrictament necessari, la Presidència de la Comissió de Seguretat ho autoritzarà encara que no s'acompleixi aquest requisit i en farà constar el motiu per escrit i adoptarà aquelles mesures necessàries per garantir un nivell adequat de seguretat. Aquesta informació s'haurà de fer constar per escrit[17].

Article 50. **Reutilització de suports**

La reutilització de qualsevol tipus de suport magnètic requereix la comprovació del bon estat físic del mateix, així com del seu formatat amb anterioritat a la gravació de la nova informació, per tal d'evitar la possible recuperació de restes de la informació continguda amb anterioritat.

D'acord amb el temps mitjà d'utilització abans d'error (de l'anglès, *Medium Time Between Fails MTBF*) indicat pel fabricant de les cintes, es procedirà a establir un registre d'ús per tal de retirar-les i destruir-les a partir d'un nombre d'utilitzacions màxim i així assegurar el correcte control de l'envelliment de les mateixes.

La Presidència de la Comissió de Seguretat adoptarà les mesures necessàries per a l'acompliment d'aquest precepte.

Article 51. **Destrucció de suports que continguin informació protegida**

Les persones Administradores de Sistemes i de Bases de Dades adoptaran les mesures necessàries per impedir qualsevol recuperació posterior de la informació emmagatzemada en els suports o documents destruïts, prèviament a què es doni de baixa de l'inventari.

La destrucció de les proves d'impressió o dels llistats de treball, en què es contingui informació relativa a persones físiques o jurídiques, es realitzarà de forma immediata, mitjançant màquina destructora, sense que, en cap cas, puguin ser dipositades en les papereres convencionals.

No està permès reutilitzar paper que en el seu anvers contingui dades de caràcter personal.

---

[17] S'hi incorpora, com a ANNEX 14, el document que conté el model d'*Autorització per a l'ús de dispositius portàtils* (PDPL25).

Article 52. **Criteris d'Arxiu dels documents**
L'arxiu dels suports o documents haurà de garantir la correcta conservació dels documents, la seva localització i la consulta de la informació.

Article 53. **Custòdia de suports en format paper**
Quan la documentació amb dades personals encara no es trobi arxivada als dispositius d'emmagatzematge establerts, per trobar-se en procés de revisió o tramitació, ja sigui previ o posterior al seu arxiu, la persona que estigui a càrrec d'aquesta haurà de custodiar-la i impedir en tot moment que hi puguin accedir persones no autoritzades.

Article 54. **Còpia o reproducció de documents**
La generació de còpies o la reproducció dels documents únicament podrà ésser realitzada sota el control del personal autoritzat. Correspon autoritzar la generació de còpies o la reproducció de documents a la persona encarregada del tractament, que utilitzarà el model d'autorització establert[18].

TÍTOL VI. CÒPIES DE SEGURETAT I RECUPERACIÓ DE DADES

CAPÍTOL I. CÒPIES DE SEGURETAT

Article 55. **Còpies de Seguretat**
La seguretat de les dades personals dels Fitxers no només suposa la confidencialitat d'aquestes sinó que també comporta la integritat i la disponibilitat de les mateixes. Per garantir aquests dos aspectes fonamentals de la seguretat és necessari que existeixin uns processos de recolzament i de recuperació que, en cas de fallada del sistema informàtic, permetin recuperar les dades.
Es designarà una persona, ja sigui l'Administradora de Sistemes i de Bases de Dades o bé una altra persona usuària expressament designada, que serà la responsable d'obtenir periòdicament una còpia de seguretat dels fitxers a efectes de recolzament i possible recuperació en cas de fallada.

[18] S'hi incorpora, com a ANNEX 15, el document que conté el model d'*Autorització per a la reproducció de documentació* (PDIN02-M1).

Diàriament, es realitzaran, per part dels Sistemes d'Informació, còpies incrementals de seguretat de tota la informació emmagatzemada en els discos dels servidors corporatius, segons el que s'indica a l'article 49.
Les incidències ocorregudes durant el procés de còpies seran registrades sobre la base d'allò que s'estableix a l'article 60 d'aquest Reglament.
S'establirà un sistema de rotació de cintes magnètiques que permeti recuperar qualsevol dels fitxers emmagatzemat als discos del sistema amb retroactivitat de 21 dies per a les còpies completes setmanals i de 7 dies per a les còpies incrementals diàries.
Les cintes de rotació s'emmagatzemaran al CPD protegit per un sistema antiincendis i en la caixa per fer l'intercanvi. Són les persones Administradores de Sistemes i de Bases de Dades les autoritzades per al seu transport i manipulació.
Setmanalment es retirarà del procés de rotació un joc complet de cintes, s'enregistrarà la informació que les identifica i es dipositaran en un edifici diferent a aquell on s'emmagatzemen els suports habitualment. Aquest procés es regirà pel procediment establert[19].
Serà responsabilitat de la persona usuària dels ordinadors personals portàtils o no connectats a la LAN corporativa o xarxa departamental la realització periòdica de còpies de seguretat i l'inventariat i l'emmagatzematge dels suports generats en lloc segur, sense perjudici d'allò que s'estableix a l'article 57 d'aquest Reglament.
La Presidència de la Comissió de Seguretat s'encarregarà de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de recolzament i recuperació de dades.
Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no es realitzaran amb dades reals, a excepció que es faci una còpia de seguretat dels fitxers i es garanteixi el nivell de seguretat corresponent al tractament realitzat, fet que s'haurà de fer constar a l'aplicació de gestió d'incidències.
Els fitxers de proves s'inclouran a l'inventari de fitxers corporatius i temporals om a fitxers temporals.
La Comissió de Seguretat podrà acordar la disminució dels períodes de temps que es regulen en aquest article.

Article 56. **Còpies de treball dels documents**

S'hauran d'elaborar còpies dels documents de treball susceptibles d'ésser manipulats durant el desenvolupament de les funcions dels treballadors per tal de garantir la seguretat i la integritat dels documents originals dels fitxers no automatitzats. En tot cas, aquests fitxers temporals, en estar ubicats a la Xarxa, estaran sotmesos al procés de còpies de seguretat que l'Ajuntament tingui habilitat.

[19] S'hi incorpora, com a ANNEX 16, el document que conté el *Procediment per a la realització de les còpies de seguretat* (PDPR03).

CAPÍTOL II. RECUPERACIÓ I INTEGRITAT DE DADES

Article 57. **Recuperació de dades**

En cas de fallada del sistema, amb pèrdua total o parcial de les dades dels fitxers, se seguirà el procediment[20], informàtic o manual, que, tot partint de la darrera còpia de recolzament i del registre de les operacions realitzades des del moment de la còpia, reconstrueixi les dades dels fitxers que es considerin afectades a l'estat en què es trobaven en un moment anterior al de la fallada. Caldrà deixar-ne constància de les dades que s'indiquen al procediment de notificació i gestió d'incidències.

Es designarà una persona, ja sigui l'Administradora de Sistemes i de Bases de Dades o un altra usuària expressament designada a aquest efecte[21], que serà la responsable d'efectuar la recuperació de les dades en cas de fallada.

Serà necessària una autorització anual de la Presidència de la Comissió de Seguretat, realitzada mitjançant l'aplicació de gestió d'incidències, per a l'execució dels procediments de recuperació de les dades.

De conformitat amb allò establert a l'article 55 d'aquest Reglament, les persones usuàries podran sol·licitar a les Administradores de Sistemes i de Bases de Dades, la recuperació dels fitxers amb indicació del seu nom d'usuària o el del grup funcional al qual pertanyin.

Article 58. **Integritat física de les dades**

La consistència i la integritat física de les dades contingudes a les Bases de Dades Corporatives es garanteix, en l'estat d'explotació, mitjançant un sistema de gestió de discos i de les eines d'integritat de les quals estigui dotat el motor de la base de dades.

[20] S'hi incorpora, com a ANNEX 17, el document que conté el *Procediment de notificació i gestió d'incidències* (PDPR04).

[21] S'hi ha incorporat, com a ANNEX 2, el procediment de *Nomenament de càrrecs* (codi PDPR01).

TÍTOL VII. SISTEMA DE GESTIÓ D'INCIDÈNCIES

Article 59. **Registre d'Incidències de Seguretat**

Es portarà un Registre d'incidències de Seguretat en el qual s'anotaran les incidències ocorregudes en el sistema de seguretat, de conformitat amb allò que s'estableix en el procediment[22] de notificació i gestió d'incidències.

El Registre d'incidències de Seguretat de l'aplicació corresponent estarà a càrrec de la Presidència de la Comissió de Seguretat.

Article 60. **Notificació d'incidents en el sistema d'informació**

La Presidència de la Comissió de Seguretat habilitarà aquest Registre d'incidències, mitjançant l'aplicació informàtica corresponent, a la disposició de totes les persones usuàries i administradores dels fitxers corporatius amb la finalitat d'enregistrar qualsevol incidència que pugui suposar un perill per a la seguretat del mateix.

Les persones usuàries que tinguin constància de qualsevol incident que pugui afectar la seguretat del sistema d'informació hauran de comunicar immediatament a la persona o a les persones designades pels Sistemes d'Informació, mitjançant els canals establerts (correu electrònic o telèfon o qualsevol altra mecanisme que es determini), les circumstàncies i els efectes de l'incident, per tal de procedir, posteriorment, al seu registre.

Les persones Administradores de Sistemes i de Bases de Dades analitzaran el problema i les possibles conseqüències en els terminis establerts en els nivells de servei i adoptaran les mesures que considerin necessàries per donar resposta a l'incident i informaran, mitjançant l'aplicació de gestió d'incidències, a la Presidència de la Comissió de Seguretat, de les mesures adoptades. Finalment, es procedirà al registre de la incidència.

El coneixement i la no notificació o registre d'una incidència per part d'una persona usuària serà considerat com una falta contra la seguretat dels Fitxers i podrà donar lloc a la incoació de l'expedient sancionador corresponent.

TÍTOL VIII. AUDITORIA DE SEGURETAT

Article 61. **Periodicitat i documentació base de l'Auditoria de Seguretat**

Amb periodicitat biennal, com a mínim, es realitzarà una Auditoria de Seguretat, amb objecte de verificar el compliment, en tots els seus termes, d'aquest

[22] S'hi ha incorporat, com a ANNEX 17, el document que conté el *Procediment de notificació i gestió d'incidències* (PDPR04).

Reglament i de la normativa aplicable, la qual prendrà com a base, com a mínim, els documents següents:

a) Albarans d'entrada i sortida de l'empresa de custòdia de les còpies de seguretat.
b) Llistat de *log* d'accés al sistema.
c) Llistat de persones usuàries amb accés del sistema.
d) Registre de Còpies de Seguretat.
e) Registre d'Incidències.
f) Inventari de Fitxers Corporatius i Temporals.
g) Implementació de Mesures Tècniques i Organitzatives.

També es realitzarà una Auditoria de Seguretat sempre que es realitzin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades amb l'objectiu de verificar-ne l'adaptació, l'adequació i l'eficàcia. Aquesta Auditoria inicia el còmput de dos anys assenyalat a l'apartat anterior.

L'auditoria de seguretat abastarà els fitxers i tractaments automatitzats i els fitxers i tractaments no automatitzats.

Article 62. **Controls periòdics de verificació del compliment**

Periòdicament, de conformitat amb les instruccions de la Comissió de Seguretat, caldrà comprovar la veracitat de les dades contingudes en els annexes d'aquest Reglament, així com el grau de compliment de les normes que conté, amb la finalitat de detectar i resoldre les anomalies que sorgeixin.

Correspon a la Presidència de la Comissió de Seguretat establir els mecanismes per a l'efectiva implantació dels controls periòdics de verificació del compliment de les mesures de seguretat. Igualment, amb una periodicitat almenys anual, comprovarà que la llista de persones usuàries autoritzades al sistema informàtic habilitat a l'efecte, es correspon amb la llista de les persones usuàries realment autoritzades a les aplicacions d'accés als Fitxers.

A més a més d'aquestes comprovacions periòdiques, l'Administradora de Sistemes i de Bases de Dades comunicarà a la Presidència de la Comissió de Seguretat, de manera immediata, qualsevol alta o baixa de persones usuàries amb accés autoritzat als Fitxers.

Es comprovarà també, almenys amb periodicitat semestral, l'existència de còpies de recolzament que permetin la recuperació dels Fitxers segons allò que s'estableix als articles 55 i 57 d'aquest Reglament.

A la vegada, i també amb periodicitat almenys semestral, les persones Administradores de Sistemes i de Bases de Dades comunicaran, a la Presidència de la Comissió de Seguretat, qualsevol canvi que s'hagi realitzat en les dades tècniques dels annexes, com per exemple canvis en el programari o maquinari, base de dades o aplicació d'accés als Fitxers, i es procedirà a l'actualització d'aquests annexes.

El Responsable de Seguretat verificarà, amb una periodicitat mínima semestral, el compliment d'allò que es determina en aquest Reglament quant a la gestió general de suports i a la recuperació de dades, en relació amb les entrades i sortides de dades, siguin per xarxa o en suport magnètic.
El Responsable dels Fitxers, juntament amb la Comissió de Seguretat, analitzarà, amb periodicitat almenys semestral, les incidències registrades en el Registre corresponent, per tal d'adoptar les mesures correctores que evitin o limitin aquestes incidències en el futur.
Correspon a la Comissió de Seguretat establir i exigir-ne el compliment dels mecanismes de control periòdic de verificació de l'acompliment de les mesures de seguretat per als fitxers i tractaments no automatitzats, amb els mateixos terminis indicats en aquest precepte per als fitxers i tractaments automatitzats.

Article 63. **Forma de realització de l'Auditoria**
Com a mínim cada dos anys es realitzarà una auditoria, externa o interna, que dictamini el correcte compliment i l'adequació de les mesures d'aquest Reglament de seguretat i de les exigències de la normativa vigent en la matèria, que identificarà les deficiències i proposarà les mesures correctores necessàries.
L'Auditoria podrà ser portada a terme amb mitjans interns o mitjançant la subcontractació de recursos externs.

Article 64. **Informe d'Auditoria**
L'informe d'Auditoria, que inclourà les dades, els fets i les observacions en què es basin els dictàmens emesos i les recomanacions proposades, tractarà, com a mínim, els aspectes següents:
a) Adequació de les mesures i controls al document i a la normativa vigent.
b) Identificació de deficiències.
c) Proposta de mesures correctores o complementàries que siguin necessàries.
Els informes d'auditoria seran analitzats per la Comissió de Seguretat, que proposarà al Responsable dels Fitxers les mesures correctores corresponents. Els informes s'hauran de conservar durant el període de temps establert.

Article 65. **Resultats de l'Auditoria**
Si del procés d'Auditoria derivessin fets que pugessin determinar responsabilitat disciplinària, patrimonial, civil o penal es procedirà a posar-ho en coneixement de l'òrgan competent, als efectes de la seva exigència.
Finalitzat el procés d'Auditoria, es procedirà a remetre comunicació a l'Agència Catalana de Protecció de Dades als efectes de posar a la seva disposició els resultats de la mateixa.

TÍTOL IX. CAPTACIÓ DE DADES DE CARÀCTER PERSONAL I EXERCICI DE DRETS

Article 66. Captació de les dades de caràcter personal

Tota captació de dades requerirà la incorporació del deure d'informació a què es refereix l'article 5 de la *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.* Serà responsabilitat de les persones encarregades del tractament que els formularis de captació de dades personals continguin una nota legal, a peu de pàgina, que acompleixi amb el dret d'informació.
La captació de dades es durà a terme tot seguint el procediment en cada moment establert[23].
Si es disposa de dades de caràcter personal emmagatzemades i que s'hagin obtingut amb omissió d'allò que es determina en l'apartat anterior, aquestes s'hauran de sotmetre al procediment de regularització de les dades en un termini màxim de sis mesos des de l'entrada en vigor d'aquest Reglament. Correspon a la persona encarregada del tractament garantir el compliment d'aquesta obligació.
Les persones usuàries hauran de garantir el correcte tractament de les dades de caràcter personal quant a l'obtenció del consentiment de la persona interessada, sobretot pel que fa a dades especialment protegides i les relatives a la salut.
Quan les dades de caràcter personal no hagin estat recollides directament de la persona interessada, aquesta haurà d'ésser informada de forma expressa, precisa i inequívoca, per part del Responsable dels Fitxers o del seu representant, dins els tres mesos següents al moment del registre de les dades, del contingut del tractament, de la procedència de les dades, així com del previst als apartats a), d) i e) de l'art. 5.1 de la LOPD; llevat dels casos que la *Ley 15/1999, de 13 de diciembre*, excepciona d'aquesta obligació.

Article 67. Exercici de drets

L'exercici dels drets d'accés, rectificació, cancel·lació i oposició per part de la ciutadania es realitzarà, gratuïtament, a través del procediment[24] establert, que en garantirà la senzillesa.
La persona encarregada del tractament garantirà, en cada àmbit funcional, l'acompliment estricte de l'esmentat procediment i l'exercici correcte dels seus drets per part de la ciutadania.

---

[23] S'hi ha incorporat, com a ANNEX 12, el document que conté el *Procediment de captació de dades de caràcter personal* (PDPR05).

[24] S'hi incorpora, com a ANNEX 18 el document que conté el *Procediment d'exercici dels drets* (PDPR08).

TÍTOL X. RELACIONS AMB TERCERES PERSONES

Article 68. **Accés a les dades per compte de terceres persones**

La realització de tractaments per compte de terceres persones es regularà pel model de contracte[25] establert, que s'ajustarà a les determinacions de l'article 12 de la LOPD.

Una vegada complerta la prestació contractual, les dades de caràcter personal hauran de ser destruïdes o retornades al Responsable dels Fitxers, a l'igual que qualsevol suport o document en què consti alguna dada personal objecte de tractament. No procedirà la destrucció de les dades quan existeixi una previsió legal que exigeixi la seva conservació. En aquest cas s'haurà de procedir a la devolució de les mateixes tot garantint el Responsable del Fitxer la seva conservació

L'Ajuntament identificarà els fitxers que es tracten per compte de terceres persones amb referència expressa al contracte o document que regula les condicions de l'encàrrec així com la identificació de l'Encarregat del Tractament i el període de vigència de l'encàrrec.

Quan les persones interessades exerceixin els seus drets davant de l'Encarregat del Tractament i sol·licitin l'exercici del/s dret/s d'accés, rectificació, cancel·lació i/o oposició, l'Encarregat del Tractament haurà de donar trasllat de la sol·licitud al Responsable del Fitxer, amb la finalitat que aquest la resolgui, llevat que al contracte s'inclogui explícitament que l'Encarregat del Tractament atendrà, per compte del Responsable, les sol·licituds d'exercici de drets.

TÍTOL XI. GESTIÓ DE L'ARXIU MUNICIPAL

Article 69. **Accés i extracció de dades**

La transferència de documentació a l'arxiu general des de les diferents unitats administratives seguirà el procediment que determini la Comissió de Seguretat, s'ajustarà als requeriments establerts per la persona responsable de l'arxiu i serà ordenada per la persona encarregada del tractament de les dades.

Igualment, l'extracció de documentació de l'arxiu requerirà acomplir els requisits establerts per la persona responsable de l'arxiu i l'autorització expressa de la persona encarregada del tractament, que s'ajustarà als models establerts.

El termini ordinari de préstec de la documentació que s'extregui de l'arxiu municipal no serà superior a un mes, però es podrà prorrogar, fins a un màxim d'un any,

[25] S'hi incorpora, com a ANNEX 19 el document que conté el *Model de contractes amb terceres persones per a la comunicació de dades* (PDIN01).

sempre que es justifiqui la necessitat i d'acord amb les instruccions dictades per la persona responsable de l'arxiu municipal.
L'entrada i sortida de documentació ha de quedar enregistrada en la base de dades de l'Arxiu Municipal.
L'Arxiu Municipal, o qualsevol altra dependència similar, estarà tancada amb clau o sota vigilància permanent.

TÍTOL XII. CREACIÓ, SUPRESSIÓ O MODIFICACIÓ DE FITXERS

Article 70. **Creació, supressió i modificació**
La creació, modificació o supressió dels Fitxers de l'Ajuntament de Cerdanyola del Vallès es realitzarà per resolució d'Alcaldia i es publicarà al diari oficial corresponent.
L'expedient corresponent es tramitarà per l'Àrea on estiguin adscrits els Sistemes d'Informació i la proposta s'hi formularà per escrit per part de les persones encarregades del tractament i s'ajustarà al model establert.
La creació, modificació o eliminació de Fitxers implicarà la necessitat d'actualitzar els documents annexos referents a la «Descripció del sistema informàtic d'accés als Fitxers», «Entorn de sistema operatiu i de comunicacions dels Fitxers», «Locals i equipaments amb Fitxers o suports que els guarden», «Procediments de control, d'accessos, suport i recuperació i gestió, «Personal autoritzat per accedir als Fitxers» i «Inventari de fitxers corporatius i temporals» i la resta que hagin sofert modificacions.

Article 71. **Inscripció dels fitxers**
Correspon a l'Àrea on estiguin adscrits els Sistemes d'Informació dur a terme les actuacions necessàries per garantir la inscripció dels fitxers conformement a la normativa aplicable.

DISPOSICIONS

Disposició addicional. **Publicitat de les modificacions reglamentàries**
Qualsevol modificació d'aquest Reglament implicarà la necessitat de registrar-la i de procedir a comunicar-ho amb caràcter general.

Disposició transitòria primera. **Inventari de fitxers i tractament no automatitzats**
En el termini de tres mesos des de l'entrada en vigor d'aquest Reglament, la Comissió de Seguretat elaborarà l'inventari dels fitxers que continguin dades de caràcter personal i que no estiguin en suport electrònic i proposarà l'adopció de les mesures que en garanteixin la protecció de dades personals i les mesures a adoptar, amb el calendari d'actuacions, per aconseguir, si resulta possible, la seva automatització

Disposició transitòria segona. **Manual de protecció de dades de caràcter personal**
En el termini de sis mesos des de l'entrada en vigor d'aquest Reglament, la Comissió de Seguretat elaborarà una «Manual de protecció de dades de caràcter personal» que consistirà en un document amb les normes bàsiques que s'haurà de facilitar a totes les persones al servei de l'Ajuntament de Cerdanyola del Vallès en el moment del seu ingrés.

Disposició transitòria tercera. **Ordenança Municipal d'Administració Electrònica**
En el termini de nou mesos des de l'entrada en vigor d'aquest Reglament, la Comissió de Seguretat elevarà a l'òrgan competent la proposta de modificació de l'Ordenança Municipal d'Administració Electrònica que permeti adaptar-la, si escau, a les prevencions d'aquest Reglament.

Disposició final. **Entrada en vigor**
Aquest Reglament entrarà en vigor als vint dies des de la seva publicació íntegra en el Butlletí Oficial de la Província de Barcelona, sempre que s'hagi publicat al Diari Oficial de la Generalitat de Catalunya l'anunci de publicació del BOPB en què se n'ha inserit el text íntegre.

RELACIÓ D'ANNEXOS.

—**ANNEX 1,** de l'*Inventari de fitxers corporatius i temporals* (codi PDPL05).

—**ANNEX 2**, el procediment de *Nomenament de càrrecs* (codi PDPR01).

—**ANNEX 3**, el document que conté la descripció dels recursos físics, identificat com a *Locals i equipaments amb Fitxers o suports que els guarden* (codi PDPL12).

—**ANNEX 4**, el document que conté la descripció dels equips informàtics integrats en la xarxa corporativa o en xarxes departamentals i l'entorn operatiu, identificat com a *Entorn de sistema operatiu i de comunicacions dels Fitxer*s (codi PDPL11).

—**ANNEX 5**, el document que conté la descripció dels sistemes informàtics corporatius o aplicacions per accedir a les dades, identificat com a *Descripció del sistema informàtic d'accés als Fitxers* (codi PDPL10).

—**ANNEX 6**, el document que conté la descripció dels procediments de control d'accessos, suport i recuperació i gestió, identificat com a *Procediments de control d'accessos, suport i recuperació i gestió* (codi PDPL14).

—**ANNEX 7**, el document que conté el model de l'*Informe del registre dels accessos a l'aplicació de control d'accessos al CPD* (codi PDPL02).

—**Annex 8**, el *Missatge d'inici de sessió* (codi PDPL24).

—**Annex 9**, el document que conté les mesures de seguretat per als fitxers no automatitzats, identificat com a *Tractaments no automatitzats de dades* (codi PDIN02)

—**Annex 10**, el document que conté el *Formulari d'alta de persona usuària a la xarxa informàtica* (codi PDPL23).

—**ANNEX 11**, el document que conté l'*Inventari del programari («software»)* (PDPL04).

—**ANNEX 12**, el document que conté el *Procediment de captació de dades* (PDPR05)

—**ANNEX 13**, el document que conté les *Instruccions sobre la cessió de dades del padró municipal d'habitants* (PDIN05).

—**ANNEX 14**, el document que conté el model d'*Autorització per a l'ús de dispositius portàtils* (PDPL25).

—**ANNEX 15**, el document que conté el model d'*Autorització per a la reproducció de documentació* (PDIN02-M1).

—**ANNEX 16,** el document que conté el *Procediment per a la realització de les còpies de seguretat* (PDPR03).

—**ANNEX 17**, el document que conté el *Procediment de notificació i gestió d'incidències* (PDPR04).

—**ANNEX 18** el document que conté el *Procediment d'exercici dels drets* (PDPR08).

—**ANNEX 19** el document que conté el *Model de contractes amb terceres persones per a la comunicació de dades* (PDIN01).

DILIGÈNCIA per fer constar que aquest Reglament s'aprovà inicialment en sessió plenària de l'Ajuntament de Cerdanyola del Vallès de data 28 de maig de 2009. Se sotmeté a informació pública i els anuncis corresponents es publicaren al BOPB núm. 144 de 17 de juny de 2009 i al DOGC núm. 5405 de 22 de juny de 2009, sense que s'hagin produït al·legacions o suggeriments; per la qual cosa, es considera definitivament aprovat.

Cerdanyola del Vallès, 31 de juliol de 2009