Document de seguretat

FITXERS DE DADES DE CARÀCTER PERSONAL AMB NIVELL DE SEGURETAT BÀSIC

NIVELL BÀSIC

FITXER DE BASE DE DADES DE CONTACTES
FITXER DE BASE DE DADES DEL DIETARI DE PAISATGE I DEL BUTLLETÍ DE PAISATG-E

Observatori del Paisatge

Divulgació del document
La versió actualitzada d'aquest document estarà publicada a la web de l'Observatori del Paisatge de Catalunya

Revisió del document
Aquest procediment ha de ser revisat com a mínim anualment pel responsable de seguretat organitzativa i jurídica.

1. Àmbit d'aplicació

El present document s'ha d'aplicar als fitxers que contenen dades de caràcter personal que estan sota la responsabilitat de l'Observatori del Paisatge de Catalunya, inclosos els sistemes d'informació, suports i equips utilitzats per al tractament de dades de caràcter personal, que han de ser protegits d'acord amb el que disposin la normativa vigent, les persones que intervenen en el tractament i els locals en què se situen.

La protecció de les dades dels fitxers pel que fa a accessos no autoritzats s'ha de fer mitjançant el control de totes les vies per les quals hom pugui tenir-hi accés. Els recursos que, pel fet de servir de mitjà directe o indirecte per accedir als fitxers, han de ser controlats per aquesta normativa són:

- Els llocs de treball i els sistemes informàtics o aplicacions, siguin locals o remots, establerts per accedir a les dades, des dels quals hom pot tenir accés als fitxers.
- Els servidors i l'entorn de sistema operatiu i de comunicacions en què estan situats els fitxers, descrits a l'**annex 4** d'aquest document.
- Els centres de tractament i els locals on estan situats els fitxers o s'emmagatzemen els suports que els continguin, la descripció dels quals figura a l'**annex 4**.
- Les còpies de seguretat, on s'emmagatzema el suport dels fitxers.

Els fitxers subjectes a les mesures de seguretat establertes en aquest document, degudament notificats davant l'Agència Catalana de Protecció de Dades i que s'adjunten a l'**annex 1**, es troben oficialment classificats[1] com a nivell bàsic

Nivell bàsic	S'aplicarà a qualsevol fitxer que contingui dades de caràcter personal, és a dir, que permetin identificar una persona: nom, cognoms, DNI, domicili, telèfon, etc.
	També als fitxers que continguin dades d'ideologia, afiliació sindical, religió, creences, salut, origen racial o vida sexual, quan: • les dades s'utilitzen amb l'única finalitat de realitzar una transferència dinerària a entitats de les quals els afectats siguin associats o membres; • es tracti de fitxers o tractaments no automatitzats o siguin tractaments manuals d'aquests tipus de dades de forma incidental o accessòria, que no guarden relació amb la finalitat del fitxer; • els fitxers o tractaments continguin dades de salut, que es refereixin exclusivament al grau o condició de discapacitat o la simple declaració d'invalidesa, amb motiu del compliment de deures públics.

[1] Segons els nivells definits al títol VIII del Reial decret 1720/2007, de 21 de desembre

2. Funcions i obligacions del personal

El present apartat recull les funcions i les obligacions a les quals està subjecte i que ha de conèixer, acceptar i seguir tot el personal de l'Observatori del Paisatge. En l'àmbit d'aquest document, sempre que es faci referència al personal, s'ha d'entendre que hom es refereix tant al personal d'administració i tècnic com al subcontractat que tingui accés als recursos de l'entitat.

Les normes que es redacten a continuació s'han d'aplicar ordinàriament a tots els fitxers que es descriuen a l'**annex 1** d'aquest document. Una còpia d'aquest document amb la part que l'afecti serà lliurada, si així ho sol·licita, per al seu coneixement, a cada persona autoritzada a accedir a les dades d'un fitxer.

Totes les persones que tinguin accés a les dades d'un fitxer tenen l'obligació, per llei, de omplir el que estableix aquest document i estan subjectes a les conseqüències en què puguin incórrer en cas d'incompliment.

2.1. Classificació del personal

A efectes d'aquesta normativa, s'estableixen uns perfils per al personal de l'Observatori del Paisatge, de manera que cadascú pertanyerà almenys a una d'aquestes categories:

- **Responsables de la informació**: a qui s'assigna la responsabilitat d'adquirir, desenvolupar i mantenir la informació. Entre altres funcions, correspon als responsables classificar la informació segons el nivell i la confidencialitat, designar els usuaris als quals és permès l'accés i aprovar i autoritzar les diverses formes en què la informació és utilitzada. Pertanyen a aquest perfil les figures següents:
  - responsable del fitxer
  - responsable de seguretat
- **Administradors informàtics**: personal tècnic que també té accés a la informació, però no per al desenvolupament de la seva feina, sinó com a encarregat de les tasques d'administració i manteniment dels sistemes d'informació de l'Observatori.
- **Usuaris de la informació**: tot el personal que hi accedeix i utilitza la informació per al desenvolupament de la seva feina habitual, i que és responsabilitat de l'Observatori.

A continuació s'especifiquen les funcions i les obligacions a les quals està subjecte el personal que pertany a cada una de les categories esmentades.

2.2. Responsables de la informació

2.2.1. Responsable del fitxer

El responsable del fitxer és l'**encarregat de la seguretat del fitxer** i d'implantar les mesures que es detallen a la normativa de seguretat de l'OPC. També adoptarà les mesures necessàries perquè els empleats coneguin les normes que tinguin a veure amb el desenvolupament de les seves funcions i que estiguin recollides al Document de seguretat.

A continuació s'enumeren les principals funcions i obligacions que adquireix el responsable del fitxer, que es detallen a l'**annex 8**.

- Normativa de seguretat
- Controls i autoritzacions
- Comunicacions amb l'Agència Espanyola de Protecció de Dades (AEPD) i els afectats
- Controls periòdics de verificació del compliment
- Responsabilitat

2.3. Administradors informàtics

Es tracta del personal que **administra els sistemes** mitjançant els quals hom accedeix als fitxers de dades.

Les principals funcions de l'administrador informàtic són les següents, que es detallen a l'**annex 8.**

- Gestió d'incidències
- Salvaguarda i protecció de les contrasenyes personals
- Procediments de còpies de seguretat i de recuperació de dades
- Proves amb dades reals
- Fitxers temporals
- Controls periòdics de verificació del compliment

2.4. Obligacions que afecten tot el personal

Tot el personal que accedeixi al fitxer ha de complir les normes de seguretat que es defineixen a continuació.

2.4.1. Llocs de treball

- Cada empleat és **responsable del seu lloc de treball.** Vetllarà perquè tant la informació que es mostri a través de la pantalla del seu ordinador com els documents en paper, etc. que utilitzi al seu lloc de treball i que continguin dades de caràcter personal **no puguin ser vistos** per persones **no autoritzades** per accedir a les dades del fitxer.

- Això implica que tant les **pantalles** com les **impressores** o un altre tipus de dispositius connectats al lloc de treball han d'estar físicament ubicats en llocs que garanteixin aquesta **confidencialitat**. Per exemple, no s'han de situar pantalles en llocs que siguin visibles per a persones externes, com ara zones de pas, finestres...

- Quan el responsable d'un lloc de treball l'**abandoni**, o bé temporalment o bé en acabar el torn de treball, l'ha de deixar en un estat que **impedeixi la visualització de les dades protegides**. Això es fa amb un protector de pantalla, que impedeix la visualització de les dades i que sol·licita la contrasenya de l'usuari per reprendre la feina. Pel que fa a la documentació en paper que conté informació sensible, es guardarà preferentment en armaris tancats amb clau o en llocs que no siguin accessibles a personal no autoritzat.

- En el cas de les **impressores**, cal assegurar que **no quedin documents impresos** a la safata de sortida que continguin **informació sensible**. Si les impressores són compartides amb altres usuaris no autoritzats per accedir a les dades del fitxer, els responsables de cada lloc han de retirar els documents a mesura que es vagin imprimint.

- Els **llocs de treball** des dels quals hom té accés al fitxer tindran una **configuració fixa** de les aplicacions i els sistemes operatius que només podrà ser canviada amb l'autorització del responsable de seguretat o pels administradors del sistema.

2.4.2. Salvaguarda i protecció de les contrasenyes personals

- El mecanisme que s'empra habitualment per validar la identitat d'una persona consisteix a assignar-li una parella, que és un codi d'usuari i una contrasenya. El codi d'usuari és públic i identifica la persona en el sistema. La contrasenya és secreta; només la pot saber la persona a qui correspon el codi d'usuari. És obligació de l'usuari mantenir la seva contrasenya en secret i tenir cura que altres no la puguin saber.

- Cada empleat amb accés als sistemes informàtics ha de tenir un nom d'usuari i una contrasenya. Aquest codi d'usuari només el pot emprar una única persona. Es prohibeix l'accés a qualsevol dels sistemes de l'OPC de forma anònima o amb el codi d'una altra persona.

- Cada usuari és responsable de la confidencialitat de la seva contrasenya. Si l'empleat sospita que la seva contrasenya pot haver estat compromesa, per qualsevol circumstància, l'ha de canviar i posar-ne una de nova. Si l'empleat s'adona que una altra persona ha tingut accés fortuïtament o fraudulentament a la seva contrasenya, ha de registrar-ho com a incidència de seguretat i canviar-la immediatament.

• L'empleat ha de verificar la darrera data de connexió que li mostra el sistema i comprovar si és la data en la qual es va connectar ell per darrera vegada. Si no coincideix o té dubtes, ha de canviar la contrasenya immediatament.

• Les contrasenyes emprades en els sistemes de l'OPC no es poden emprar en altres sistemes, llocs o àmbits. Les contrasenyes emprades en els sistemes de l'OPC han de ser úniques, creades expressament per a l'autenticació que es requereix a l'OPC. Les contrasenyes no poden ser reutilitzades. Tampoc no s'han d'escriure o introduir en cap pantalla, formulari o pàgina que no sigui l'habitual per autenticar-se en el sistema corresponent.

• Davant una baixa o absència temporal prolongada d'un usuari, el responsable del fitxer pot autoritzar que hi accedeixi un altre usuari amb la temporalitat i els permisos que es considerin necessaris.

2.4.3. Gestió d'incidències

• **Qualsevol usuari** que tingui coneixement d'una **incidència** ho ha de **comunicar immediatament a l'administrador del sistema**. Aquesta comunicació s'ha de fer en un termini no superior a un dia laboral des que es tingui coneixement de la incidència.

• S'entén per **incidència** qualsevol situació o esdeveniment que afecti o pugui afectar la seguretat, la integritat i/o la disponibilitat de les dades. Alguns exemples d'incidències podrien ser: infecció per virus d'un arxiu o d'una aplicació, enviament d'informació personal a una adreça equivocada, donar informació sensible a persones alienes, avaria de disc dur que provoqui pèrdua de dades, caiguda de la xarxa informàtica, etc.

• El fet que un usuari conegui i no notifiqui una incidència serà considerat com una falta contra la seguretat del fitxer per part d'aquest usuari.

2.4.4. Qualitat de les dades[2]

• No es permet recollir dades personals sense l'autorització expressa d'un responsable de fitxer nomenat.

• Les dades de caràcter personal només es poden recollir per a la consecució de la finalitat del fitxer en què s'inclouen i no poden utilitzar-se per a finalitats distintes d'aquelles per a les quals s'hagin recollit.

• Les dades de caràcter personal han de ser exactes i estar posades al dia, de manera que corresponguin amb veracitat a la situació actual de l'interessat. Si resulten inexactes o incompletes, s'han de cancel·lar i substituir per les correctes. Això no significa que l'OPC hagi de validar les dades de forma periòdica, sinó que, si l'interessat exerceix el dret de rectificació, les seves dades s'han de modificar adequadament.

• Les dades de caràcter personal s'han de cancel·lar quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual s'hagin recollit. Per això, cal fixar una vigència de les dades, període després del qual les dades es cancel·laran i eliminaran.

• No es permet encreuar informació relativa a dades de diferents fitxers o serveis per establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sense l'autorització expressa del responsable del fitxer.

• No es pot desenvolupar cap activitat que no estigui expressament permesa en aquest document o a les normes sobre protecció de dades i instruccions de l'Agència Espanyola de Protecció de Dades (AEPD).

2.4.5. Informació i autorització prèvia a la recollida de dades personals[3]

• Els usuaris han de recollir únicament les dades de caràcter personal relatives als fitxers declarats per l'OPC, l'estructura dels quals es descriu a l'**annex 1** d'aquest Document de seguretat.

• Els interessats als quals se sol·liciten dades personals han de ser prèviament informats:

[2] LOPD, article 4.
[3] LOPD, article 5.

a. De l'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la recollida d'aquestes i dels destinataris de la informació.
b. Del caràcter obligatori o no de les seves respostes a les preguntes que els siguin plantejades.
c. De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
d. De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
e. De la identitat i l'adreça del responsable del tractament.

• No és necessària la informació a què es refereixen les lletres b) i c) de l'apartat anterior si el contingut es dedueix clarament de la naturalesa de les dades personals que se sol·liciten o de les circumstàncies en què es recullen.

2.4.6. Deure de secret[4]

• Tots els usuaris estan obligats al **secret professional** respecte de les dades de caràcter personal i al deure de guardar-les, obligacions que **subsistiran encara després de finalitzar** les relacions amb el titular del fitxer o, en el seu cas, amb el responsable del fitxer.

2.4.7. Confidencialitat de la informació

• Està **prohibit enviar informació confidencial** de l'OPC a l'exterior, mitjançant suports materials o a través de qualsevol altre mitjà, sense l'**autorització** expressa del seu responsable.

• Cap usuari no pot revelar informació confidencial adquirida per raó de la seva posició, ni utilitzar d'una altra manera aquesta informació per al seu guany o benefici personal.

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

• En cas que l'usuari entri en possessió d'informació confidencial, s'ha d'entendre que aquesta possessió és estrictament temporal; té obligació de secret i no té cap dret de possessió o de titularitat o de còpia sobre aquesta informació. Així mateix, el treballador ha de tornar el material que contingui la informació a l'OPC, immediatament després de la finalització de les tasques que n'han originat l'ús temporal i, en qualsevol cas, quan acabi la relació laboral.

2.4.8. Gestió de suports

• Els suports que continguin dades de caràcter personal han d'estar clarament **identificats** amb una **etiqueta** externa que indiqui el tipus d'informació que contenen.

• S'han de posar els mitjans necessaris per a la **protecció** dels suports que continguin dades de caràcter personal. En acabar la jornada laboral, els suports amb dades de caràcter personal s'han d'emmagatzemar de forma que no estiguin a l'abast de personal no autoritzat, com per exemple en armaris protegits amb clau.

• S'han d'utilitzar els mitjans necessaris per **esborrar la informació** amb dades de caràcter personal dels suports abans d'eliminar-los o reutilitzar-los, de manera que no pugui ser recuperada. Així:
  - Per a la informació en **suport paper** s'han d'utilitzar **màquines de destruir documentació** habilitades a l'efecte.
  - En el cas dels **suports electrònics**, s'han de lliurar a l'**àrea d'informàtica**, on s'han de formatar i s'han de dipositar en màquines de destruir suports electrònics.

2.4.9. Propietat intel·lectual i industrial

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

[4] LOPD, article 10.

2.5. Conseqüències de l'incompliment del Document de Seguretat

L'incompliment d'aquestes normes es regula pel que disposa la Llei 7/2007, de 12 d'abril, de l'Estatut bàsic de l'empleat públic (BOE. núm. 89, de 13 d'abril), sens perjudici d'altres responsabilitats que hi pugui haver.

Els responsables de serveis i unitats han de vetllar per l'efectiu compliment del que disposa la present normativa, i promoure accions de sensibilització, divulgació i implantació entre el personal a càrrec seu.

2.6. Obligacions d'un encarregat del tractament

Segons el que estableix l'article 3.g) de la LOPD, s'entén per encarregat del tractament: «la persona física o jurídica, l'autoritat pública, el servei o qualsevol altre organisme que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament». Aquesta realització de tractament per compte de tercers ha d'estar **regulada en un contracte** que ha de constar per escrit o en alguna altra forma que permeti acreditar-ne la subscripció i el contingut, i s'hi ha d'establir expressament que l'encarregat de tractar les dades ho farà d'acord amb les instruccions del responsable del fitxer, que no les aplicarà o utilitzarà amb finalitats distintes de les que figurin al contracte, ni les comunicarà, ni tan sols per a la conservació, a altres persones.

No es considera encarregat del tractament la persona física que tingui accés a les dades personals en la seva condició d'empleat dins la relació laboral que manté amb el responsable del fitxer.

3. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat dels fitxers

Les normes que es descriuen al present apartat s'han d'aplicar ordinàriament a tots els fitxers declarats per l'OPC, categoritzats com a **bàsics**.

De la mateixa manera, al llarg del document, s'indica quan les **mesures** són específiques per aplicar a **fitxers informatitzats o automatitzats** i als **manuals o no automatitzats** (en suport paper). En cas que no es faci cap indicació, les mesures s'han d'aplicar amb caràcter general, tant a fitxers automatitzats com no automatitzats.

3.1. Resum

A continuació es mostra una taula resum de les mesures que cal adoptar en cada un dels fitxers:

Personal	— Funcions i obligacions dels diferents usuaris o dels perfils d'usuaris clarament definides i documentades. — Definició de les funcions de control i les autoritzacions delegades pel responsable — Difusió entre el personal de les normes que els afectin i de les conseqüències per incompliment
Incidències	— Registre d'incidències: tipus, moment de detecció de la incidència, persona que la notifica, efectes i mesures correctores — Procediment de notificació i gestió de les incidències
Control d'accés	— Relació actualitzada d'usuaris i accessos autoritzats — Control d'accessos permesos a cada usuari segons les funcions assignades — Mecanismes que evitin l'accés a dades o recursos amb drets distints dels autoritzats — Concessió de permisos d'accés només per a personal autoritzat — Les mateixes condicions per a personal aliè amb accés als recursos de dades
Identificació i autenticació	**Només fitxers automatitzats** — Identificació i autenticació personalitzada — Procediment d'assignació i distribució de contrasenyes — Emmagatzematge inintel·ligible de les contrasenyes — Periodicitat del canvi de contrasenyes (< 1 any)
Gestió de suports	— Inventari de suports — Identificació del tipus d'informació que contenen, o sistema d'etiquetatge — Accés restringit al lloc d'emmagatzematge — Autorització de les sortides de suports (incloses a través d'e-mail). — Mesures per al transport i l'eliminació de suports
Còpies de seguratat	**Només fitxers automatitzats** — Còpia de seguretat setmanal — Procediments de generació de còpies de seguretat i recuperació de dades — Verificació semestral dels procediments — Reconstrucció de les dades a partir de la darrera còpia — Proves amb dades reals: còpia de seguretat i aplicació del nivell de seguretat corresponent
Criteris d'arxiu	**Només fitxers no automatitzats** — L'arxiu dels documents s'ha de realitzar segons criteris que en facilitin la consulta i localització per garantir l'exercici dels drets ARCO
Emmagatzematge	**Només fitxers no automatitzats** — Dispositius d'emmagatzematge dotats de mecanismes que n'obstaculitzin l'obertura
Custòdia de suports	**Només fitxers no automatitzats** — Durant la revisió o tramitació, la persona a càrrec dels documents ha de ser diligent i custodiar-los per evitar accessos no autoritzats

- Els accessos a través de xarxes de telecomunicacions han de garantir un nivell de seguretat equivalent al dels accessos en mode local.
- L'execució de feines fora dels locals del responsable o de l'encarregat del tractament, l'autoritza prèviament el responsable del fitxer i ha de garantir el nivell de seguretat.
- Els fitxers temporals han de complir el nivell de seguretat corresponent i s'han d'esborrar una vegada que hagin deixat de ser necessaris.
- L'accés facilitat a un encarregat de tractament ha de constar al Document de seguretat, i aquesta persona s'ha de comprometre a complir les mesures de seguretat previstes.

3.2. Normativa sobre els principis de protecció de dades

3.2.1. Qualitat de les dades[5]

Les dades personals que es recullen han de ser **adequades, pertinents** i **no excessives** en relació amb l'àmbit i la finalitat per a les quals s'hagin obtingut. Per tant:

• La recollida de dades **no s'ha de fer per mitjans deslleials, fraudulents** o en forma contrària a les disposicions de la normativa vigent.

• Les dades objecte de tractament **no s'han d'utilitzar** per a una **finalitat distinta** d'aquella que n'hagi motivat l'obtenció.

• Les dades han de ser **exactes**, s'han d'actualitzar en cas que sigui necessari, i només es poden alterar amb l'autorització expressa de l'afectat.

• Les dades que siguin **inexactes o incompletes**, el responsable del fitxer **les ha de suprimir** o, si escau, **completar** quan tingui coneixement de la inexactitud o del caràcter incomplet de la informació de què es tracti, de manera que el contingut respongui a la situació actual de l'afectat.

• **No s'han de registrar** a l'OPC **dades l'origen o la qualitat de les quals no estiguin garantits** o si no les ha facilitades l'afectat a través dels contractes o **formularis establerts per a la recollida de dades.**

• Les dades s'han d'**emmagatzemar** de manera que permetin l'exercici dels drets de l'afectat.

• Hom **ha de cancel·lar** les dades de caràcter personal quan deixin de ser **necessàries o pertinents per a la finalitat** per a la qual s'hagin recollit. Només es poden conservar en els casos en què els afectats hi hagin atorgat el consentiment.

També es conservaran les dades si hi ha una llei que obligui a emmagatzemar-les.

Aquestes dades no es poden conservar per períodes superiors als necessaris marcats per l'esmentada normativa, i s'han d'arxivar en fitxers immobilitzats, que no s'utilitzaran amb cap altra finalitat.

3.2.2. Dret d'informació en la recollida de dades[6]

Quan es recullen dades personals, cal **informar-ne** prèviament els titulars de forma expressa i clara.

En el moment de recollir les dades de caràcter personal, hom notificarà a l'afectat:

• L'**existència d'un fitxer** amb les seves dades, la **finalitat** de la recollida de les dades i els **destinataris** de la informació.

• El **caràcter obligatori o facultatiu de les respostes**, així com les **conseqüències** de l'obtenció de les dades o de la negativa a subministrar-les.

• La possibilitat d'exercir els **drets d'accés, rectificació, cancel·lació i oposició** de les seves dades.

• El **responsable de les dades i l'adreça** on pot exercir el dret d'accés, rectificació, cancel·lació i supressió de les seves dades.

No es pot registrar cap dada de caràcter personal fins que no s'hagi atorgat a l'afectat el dret a la informació. En els casos de dades que provinguin de fonts accessibles al públic i amb la finalitat de publicitat, cada comunicat que s'enviï a l'afectat ha d'indicar el dret a la informació, i a més, s'ha d'indicar l'origen de les dades.

[5] Article 4 de la LOPD i article 8 i següents del RDLOPD.
[6] Article 5 de la LOPD i article 18 del RDLOPD.

3.2.3. Consentiment de l'afectat (exprés/tàcit)[7]

L'afectat és el vertader propietari de les dades personals i, per tant, ha d'**atorgar el seu consentiment** per al tractament. S'ha de demanar el **consentiment exprés per escrit** quan es recullen **dades sensibles**, és a dir, aquelles que puguin afectar de forma determinant la intimitat de la persona (**ideologia, creences, religió, origen racial, salut, vida sexual** o **derivats de violència de gènere**). En el cas de **dades de menors**, el consentiment ha de ser **exprés** i l'ha d'atorgar el **responsable legal** del menor. No es poden registrar dades de menors sense el consentiment del responsable.

En els casos en què sigui necessari el consentiment exprés, no es pot utilitzar cap formulari/contracte o similar sense la firma de l'afectat. **L'afectat pot revocar el seu consentiment en qualsevol moment**. La revocació **no té efectes retroactius** (llevat de normativa encontra), per tant, el tractament automatitzat de les dades personals de l'afectat realitzat amb anterioritat a la revocació del consentiment és vàlid.

3.2.4. Dades especialment protegides

Es consideren dades especialment protegides les dades d'**ideologia, afiliació sindical, creences o religió**. Aquestes dades sempre s'han de recollir amb el **consentiment exprés (per escrit)** de l'afectat.

En cas que es consideri necessari emmagatzemar aquest tipus d'informació, s'ha de classificar com a tal i s'han d'establir els controls pertinents. En qualsevol cas, abans de la creació d'un fitxer d'aquest tipus, s'ha de consensuar amb el responsable de seguretat i/o amb la Secretaria General, que verificarà l'absència de normativa específica que prohibeixi la recopilació de les esmentades dades; sempre s'ha de demanar el consentiment exprés de l'afectat, i no es pot utilitzar cap dada personal fins que no es tingui el dit consentiment.

3.2.5 Dades de menors[8]

Es pot procedir al tractament de les dades dels **més grans de catorze** (14) **anys** amb **el seu consentiment**, llevat d'aquells casos en què la Llei exigeixi per a la prestació l'assistència dels titulars de la pàtria potestat o tutela, i d'acord amb el que preveuen l'article 3 de la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge (BOE núm. 115, de 14 de maig), i l'article 162 del Codi Civil. En el cas dels **menors de catorze anys**, es requereix el **consentiment dels pares o tutors**.

En cap cas no es poden recollir del menor, dades que permetin obtenir informació **sobre els altres membres del grup familiar sense el consentiment dels titulars** de les dades. No obstant això, es poden recollir les **dades d'identitat i adreça** del pare, la mare o el tutor amb **l'única finalitat de recollir l'autorització** prevista a l'apartat anterior. Està **prohibit** utilitzar el menor per obtenir dades innecessàries sobre la resta de la família, com els ingressos, les preferències d'oci, etc.

Quan el tractament es refereix a dades de menors de edat, la informació dirigida a aquests s'ha d'expressar en un **llenguatge que els sigui fàcilment comprensible**.

3.2.6. Eliminació de dades obsoletes

Periòdicament s'han d'eliminar les dades que hagin quedat obsoletes.

Es consideren *dades obsoletes*:

• Les dades d'afectats amb els quals hagi **acabat la relació contractual**, llevat que hagi estat prèviament atorgat el consentiment per al manteniment posterior, cas en què s'ha d'indicar la finalitat amb què es conserven.

• En els casos en què per **motius legals** sigui necessari **mantenir-les**, hom **marcarà** les dades com a eliminades i posteriorment les eliminarà, una vegada hagi expirat el termini establert per conservar-les.

[7] Article 6 de la LOPD i article 12 i següents del RDLOPD.
[8] Article 13 del RDLOPD.

• Les dades respecte a les quals **hagi expirat el termini màxim per emmagatzemar-les** establert per la llei (si n'hi ha).

• Aquelles respecte a les quals hagi **acabat la finalitat** per a la qual es varen recollir.

En les **prestacions de servei** en què l'OPC ha de lliurar dades de caràcter personal per a l'execució, s'ha d'incloure una **clàusula al contracte** en la qual s'indiqui que és obligatori **eliminar** les dades que s'hagin obtingut com a conseqüència d'una prestació de serveis, una vegada **finalitzada** aquesta, llevat que contractualment s'autoritzi expressament mantenir-les, en previsió de futurs serveis.

3.2.7 Cessió de dades personals

Les dades de caràcter personal objecte de tractament només es poden cedir per al compliment de **fins directament relacionats** amb les funcions legítimes del cedent i del cessionari, amb el **consentiment previ de l'afectat**.

Si es preveu cedir les dades personals recollides, l'afectat ha de ser **informat prèviament**, durant la recollida de les dades, de la **finalitat** i del **destinatari** de la cessió. Això suposa que si el responsable del fitxer projecta cedir les dades personals recollides, ha d'informar l'afectat de la finalitat de la recollida, així com del destinatari de la cessió.

Mai no es poden cedir dades **sense el consentiment de l'afectat**. Aquest consentiment té **caràcter revocable**.

Quan l'OPC cedeixi dades de caràcter personal, el **cessionari** quedarà obligat **contractualment** a la **protecció** de les dades personals que li siguin cedides. Només es poden compartir dades personals entre entitats jurídiques distintes si la relació està formalitzada per un **contracte de prestació de serveis** degudament formalitzat o si existeix alguna **llei** que ho autoritzi.

3.2.8. Finalitat dels fitxers

Està **prohibit** utilitzar el fitxer per a una **finalitat distinta** de la que en un principi s'havia previst per a l'obtenció de les dades de caràcter personal. Davant un canvi de finalitat en el tractament de les dades, cal el consentiment de l'afectat.

3.3. Identificació i autenticació (fitxers automatitzats)

El responsable del fitxer aprovarà un mecanisme que permeti d'identificar de forma inequívoca i personalitzada tot usuari que intenti accedir al sistema d'informació i de verificar que hi està autoritzat.

El sistema que utilitza l'OPC per identificar i autenticar els usuaris autoritzats que accedeixin al sistema es detalla a l'**annex 6**.

3.4. Control d'accés

El sistema que utilitza l'OPC per limitar l'accés a les diferents àrees del sistema en funció dels privilegis de cada usuari, es detalla a l'**annex 6**.

3.5. Gestió de suports i documents[9]

La gestió de suports i documents va a càrrec de les dues entitats que custodien els fitxers protegits: l'àrea d'informàtica de l'Ajuntament d'Olot i l'empresa Serveisweb.

[9] Articles 92, 97 i 101 del RDLOPD.

3.6. Còpies de seguretat (fitxers automatitzats)

L'àrea d'informàtica de l'Ajuntament d'Olot, que té atribuïdes les tasques d'administració dels sistemes d'informació de l'OPC, és l'organisme que s'encarrega de fer les còpies de seguretat en els sistemes que estan dins el seu àmbit d'actuació.

La normativa que regeix les còpies de seguretat (fitxers automatitzats) és a l'**annex 7**.

3.7. Incidències de seguretat

L'àrea d'informàtica de l'Ajuntament d'Olot, que té atribuïdes les tasques d'administració dels sistemes d'informació de l'OPC, és l'organisme que s'encarrega de gestionar les incidències de seguretat.

3.7.1. Responsabilitats

Tot empleat o col·laborador, en funció de les atribucions que té conferides, ha de conèixer les accions o mesures a adoptar en cas de la identificació d'un incident.

Les responsabilitats relacionades amb la gestió d'incidències han d'estar degudament documentades, entre d'altres, per a cada una de les àrees següents:

- Usuaris
- Personal de tecnologies de la informació i la comunicació (personal de l'Àrea d'informàtica de l'Ajuntament d'Olot i el personal a càrrec de l'empresa Serveisweb)
- Responsable de fitxer

3.7.2. Notificació d'incidents de seguretat

Qualsevol incidència de seguretat s'ha de **notificar immediatament**, d'acord amb els procediments de notificació establerts a l'**annex 9** d'aquest document. La implantació de mesures correctores ha de ser aprovada i sol·licitada per personal autoritzat.

Tots els **empleats afectats** per un incident han de ser **informats** de la **incidència** i de les accions preses per resoldre-la. La possible **notificació a terceres parts** ha de ser **aprovada prèviament** pel responsable de seguretat. La informació manejada en la gestió i resolució de l'incident s'ha classificar degudament, d'acord amb el que estableixi la normativa de classificació i tractament d'informació.

Tot incident significatiu i persistent que pugui comprometre les dades de caràcter personal pel que fa a la confidencialitat (accés de persones no autoritzades), la integritat (que hagin estat modificades sense autorització, sigui de manera intencionada o fortuïta) o la disponibilitat (que o bé les dades o bé els sistemes que les suporten no estiguin disponibles quan hom pretén accedir-hi), s'ha de notificar immediatament.

A continuació s'indiquen alguns tipus d'incidents a tall d'exemple, i sense que la relació sigui exhaustiva:

- **Accés no autoritzat**: Tot intent d'accés no autoritzat, reeixit o no, o tota sospita d'accés no autoritzat.

- **Identificació de codis maliciosos**: A més de programació maliciosa en les aplicacions, s'hi inclouen els virus, troians o cucs.

- **Atacs d'interrupció de servei**: Supòsits d'interrupció de servei (reeixits o no) que afectin o amenacin un servei crític o la disponibilitat d'accés a gran part de la xarxa.

- **Escaneigs o proves**: Escaneigs no autoritzats de les xarxes, proves o atacs de negació de servei.

- **Pèrdues d'integritat** en els sistemes, bases de dades i xarxes.

- **Avaries en els sistemes d'informació**.

- **Errors en els enviaments d'informació a l'hora de seleccionar-ne el destinatari.**

- **Pèrdua de suports amb dades personals.**

La notificació de l'incident implica **documentar-lo** de manera que es detalli el **moment en què es produeix**, la **persona que el detecta**, **persona que efectua i persona que rep la notificació**, els **efectes o impacte** i una breu **descripció de l'incident**.

3.8. Transmissions de dades a través de xarxes de comunicacions (fitxers automatitzats)

• És important tenir en compte que els correus electrònics que continguin dades de caràcter personal, o bé al cos del missatge o bé en fitxers adjunts, formen part de fitxers de dades de caràcter personal, i per tant és fonamental tenir en compte on quedarà emmagatzemat el correu després de l'enviament o de la recepció.

• Cal establir **procediments de control de les empreses externes** que es **connectin als sistemes d'informació** de l'OPC, que prèviament hagin estat **autoritzades pel responsable el fitxer** o persona que delegui.

3.9. Proves amb dades de caràcter personal (fitxers automatitzats)[10]

•L'**entorn d'explotació** i el de **proves** i **desenvolupament** s'han de mantenir totalment **diferenciats**. No es pot accedir, de manera directa, a explotació des de l'entorn de desenvolupament. En cas que sigui necessari accedir a l'entorn d'explotació, per part de desenvolupament, per realitzar tasques de manteniment o d'altre tipus, s'ha de tenir l'**autorització** del **responsable del fitxer** (o persona que delegui).

• Com a regla general, en els **entorns de proves i desenvolupament** les **proves** dels programes i processos s'han de fer utilitzant bases de dades i fitxers amb **dades fictícies**. No obstant això, es **poden prendre dades d'explotació** per fer proves, sempre que ho **autoritzi el responsable del fitxer** (o persona que delegui), adoptant les mesures de seguretat següents:

- **Limitar l'accés lògic i físic** a aquestes dades, exclusivament, al personal autoritzat al Document de seguretat.
- Fer-ne una **còpia de seguretat abans** de la realització de les proves.
- Les dades reals provinents d'explotació s'han de sotmetre a un procés que permeti la **dissociació de les dades**, de tal manera que s'impossibiliti l'associació de la informació obtinguda amb una persona.
- **Si les dades no es dissocien,** cal **assegurar el nivell de seguretat corresponent** a la naturalesa de les dades que es manejaran.

• **Una vegada fetes les proves,** s'han d'**esborrar les dades** utilitzades.

3.10. Fitxers temporals[11]

• Els fitxers temporals o còpies de documents creats exclusivament per a feines temporals o auxiliars, **han de complir el nivell de seguretat** que els correspongui.

• Aquests fitxers es dipositen en un **directori del servidor de xarxa,** en una carpeta d'accés restringit a un usuari o un grup concret d'usuaris.

[10] Article 94.4 del RDLOPD.
[11] Article 87 del RDLOPD.

• Una vegada que hagin deixat de ser necessaris per als fins que en motivaren la creació, **els ha d'esborrar** físicament l'usuari que els va sol·licitar o l'administrador del sistema, a petició d'aquell.

• Aquests fitxers temporals **no poden ser copiats en suports externs,** ni es permetrà que surtin fora dels locals on se'n fa el tractament, llevat d'autorització expressa i per escrit del responsable del fitxer o persona que delegui.

3.11. Accés a les dades per compte de tercers

• La **informació interna** de l'OPC ha d'estar **protegida contra la difusió a terceres persones.**
• Només **es pot permetre l'accés** a la informació interna de l'OPC quan hi hagi una **necessitat de coneixement demostrable**, quan ho **exigeixi un procés administratiu o penal**, quan s'hagi signat un **acord de confidencialitat** o quan hagi estat a**utoritzat expressament pel responsable del fitxer**.

• En els **contractes** que se subscriguin entre l'OPC i empreses prestadores de serveis i que suposin el lliurament de dades de caràcter personal s'hi han d'incloure **clàusules** relatives a:

- **Deure de secret** i **confidencialitat.**
- **Prohibició de venda o cessió de les dades**.
- Tractament de les dades: s'ha d'**especificar** de forma clara i concisa la **finalitat** per a la qual es lliuren les dades i el servei que hom prestarà.
- Descripció de les **mesures de seguretat** que ha d'adoptar l'entitat en funció del nivell de les dades necessàries per a la prestació del servei.
- Obligació d'**esborrar les dades** quan no siguin necessàries i quan finalitzi la relació contractual, llevat que el responsable del fitxer, en previsió de futurs negocis, n'autoritzi expressament la conservació.

• En cas d'haver contractat la prestació de serveis per tercers per a determinats fitxers, a l'**annex 4** cal fer constar aquesta circumstància, tot indicant una **referència al contracte** i la **vigència**, així com als **fitxers** objecte del tractament.[12]

• Els qui, por compte de tercers, prestin serveis de tractament automatitzat de dades de caràcter personal **no poden aplicar o utilitzar** les obtingudes amb **finalitat distinta** de la que figuri al contracte de serveis, ni cedir-les, ni tan sols per a la conservació, a altres persones.

• **Una vegada complida la prestació contractual,** les dades de caràcter personal tractades s'han de **destruir,** llevat que hi hagi autorització expressa d'aquell per compte del qual es presten els serveis, perquè raonablement hom presumeixi la possibilitat d'ulteriors encàrrecs i, en aquest cas, es podran emmagatzemar amb les degudes condicions de seguretat per un període de cinc anys.

3.12. Règim de treball fora dels locals de la ubicació del fitxer[13]

• Si les dades personals s'han d'emmagatzemar en **dispositius portàtils** o tractar **fora dels locals de l'OPC** o de l'encarregat de tractament, hi ha d'haver una **autorització prèvia del responsable del fitxer**.

• En tot cas cal garantir el nivell de seguretat corresponent al tipus de fitxer tractat.

3.13. Control del Document de seguretat

Es distingeixen dues fases de control del Document de seguretat:

[12] Article 88.5 del RDLOPD.
[13] Article 86 del RDLOPD.

3.13.1. Revisió

El Document de seguretat es revisarà almenys una vegada l'any, o sempre que es produeixin les situacions següents:[14]

- Que apareguin nous fitxers
- Que hi hagi canvis rellevants en els sistemes d'informació o en els sistemes de tractament utilitzats
- Que hi hagi canvis organitzatius que afectin la seguretat dels fitxers
- Que hi hagi canvis en el contingut de la informació inclosa als fitxers o tractaments
- Que hi hagi canvis a les normatives o els procediments de l'OPC
- Que hagin sorgit canvis en la legislació vigent
- Que apareguin nous escenaris de riscs que no s'haguessin previst fins al moment
- Que es produeixin canvis tecnològics significatius a la plataforma de sistemes o les xarxes de comunicació
- Qualsevol altra situació no prevista que afecti la seguretat dels fitxers

El Document de Seguretat resultant serà revisat pel responsable de fitxer. En el procés hi pot participar qualsevol altre responsable o tècnic que faci falta per qüestions tècniques o administratives.

3.13.2. Aprovació

El Document de seguretat ha de passar una aprovació preliminar del Director de l'Observatori, prèvia a l'aprovació definitiva del Consell Rector.

Les modificacions del Document de seguretat han de passar una aprovació preliminar del Director de l'Observatori, prèvia a l'aprovació definitiva del Consell Rector.

[14] Article 88.7 del RDLOPD.

ANNEX 1 - FITXERS NOTIFICATS EN EL REGISTRE GENERAL DE PROTECCIÓ DE DADES

S'adjunta una relació dels Fitxers inscrits en el Registre General de Protecció de Dades de la Agència Catalana de Protecció de dades, així com la seva estructura.

FITXERS

1. FITXER DE BASE DE DADES DE CONTACTES
2. FITXER DE BASE DE DADES DEL DIETARI DE PAISATGE I DEL BUTLLETÍ DE PAISATG-E

ESTRUCTURA DELS FITXERS

FITXER DE BASE DE DADES DE CONTACTES

- Entitat / empresa
- Tipus entitat
- Departament
- Càrrec
- Idioma preferit (desplegable dels 4 idiomes)
- Cognoms
- Nom
- Professió (desplegable)
- Adreça
- CP
- Població
- Província
- País
- Regió
- Telèfon empresa fix
- Telèfon mòbil
- Telèfon particular
- Fax
- Web
- Adreça electrònica
- Adreça electrònica 2
- Observacions
- Data alta i data modificació (camps automàtics)
- Assignacions

FITXER DE BASE DE DADES DEL DIETARI DE PAISATGE I DEL BUTLLETÍ DE PAISATG-E

- Nom
- Cognoms
- Adreça electrònica
- Idioma

ANNEX 2 – ENCARREGATS DE TRACTAMENT

En el present annex es descriuen totes les prestacions de serveis que impliquen l'accés als fitxers per part de tercers, com a proveïdors de l'OPC, que actuen com encaregats de tractament.

Tots aquests tractaments es realitzen complint les exigències de l'article, 12 de la LOPD i en el Capítol III (art. 20, 21 i 22) del Reial decret 1720/2007.

Proveïdors de l'Observatori del Paisatge:

Denominació	Serveis prestats	Accés a fitxers
Serveisweb	Allotjament bases de dades, Web i correu electrònic	FITXER DE BASE DE DADES DEL DIETARI DE PAISATGE I DEL BUTLLETÍ DE PAISATG-E
Àrea informàtica Ajuntament d'Olot	Serveis informatics, allotjament bases de dades	FITXER DE BASE DE DADES DE CONTACTES

ANNEX 3 – DESCRIPCIÓ, FINALITAT I ESTRUCTURA DELS SISTEMES INFORMÀTICS D'ACCÉS ALS FITXERS

1. **Ubicació dels servidors i fitxers protegits**
   Els fitxers referenciats a l'Annex A es troben allotjats en dues ubicacions diferents. En el cas del fitxer de contactes, es troba als sistemes informàtics situats a l'Ajuntament d'Olot i en el cas del fitxers de subscriptors es troba allotjat als servidors de l'empresa Serveisweb.

LOCAL	ÀREA	SERVIDOR	S.O.	FITXERS
Ajuntament d'Olot	Àrea d'informàtica	www.olot.local	Unix	FITXER DE BASE DE DADES DE CONTACTES
Serveisweb	Cloud	opaicat.dnssw.net	Linux	FITXER DE BASE DE DADES DEL DIETARI DE PAISATGE I DEL BUTLLETÍ DE PAISATG-E

2. **Descripció dels sistemes informàtics**
   L'OPC està considerat com una entitat més dins la xarxa de l'Ajuntament d'Olot i es regeix pels seus criteris i requeriments de seguretat. Els fitxers són tractats des de les terminals informàtiques convencionals (PC i Portàtils), totes connectades a la xarxa local i corporativa de l'Ajuntament d'Olot.

3. **Sistemes d'organització i tractament de les dades**
   Tots els usuaris disposen d'un nom d'usuari i una contrasenya individual amb perfils d'accés en funció de la feina desenvolupada.

   Les terminals informàtiques tenen una ubicació individualitzada per usuari, i el seu accés està controlat per un responsable, i només els usuaris autoritzats en l'annex 5 tenen accés.

   Els accessos als fitxers estan restringits en funció de perfils d'accés segons el lloc ocupat en l'empresa i la tasca desenvolupada. La informació no continguda en aplicacions específiques (ofimàtica), es guarden en carpetes comuns per a tots els usuaris de l'OPC amb accés, totes ubicades en els servidors de dades.

   Exclusivament el personal de l'àrea d'informàtica té accés a tots els sistemes informàtics.ç

4. **Distribució dels recursos**
   En l'àrea pública l'OPC disposa d'un portal Web en què es presenta a la comunitat internacional informació sobre l'entitat i les activitats que realitza. A les àrees privades només es pot accedir mitjançant la corresponent identificació amb login i password, establint aleshores els controls de seguretat propis de l'àrea privada . L'adreça d'accés a les àrees privades no és pública.

ANNEX 4 – CONTROL D'ACCÉS ALS LOCALS I LLOCS DE TREBALL

L'OPC desenvolupa la seva activitat principal a les oficines de la seva seu tècnica situada al C/Hospici, 8 d'Olot.

En aquestes oficines, estan obligats a complir la normativa descrita a continuació:

1. Control d'accés físic
Únicament el personal autoritzat pot tenir accés a:

- Els despatxos on es trobin situats informes d'usuaris i personal de l'organització i on es trobin instal·lats ordinadors personals amb accés a les dades de caràcter personal.
- El personal extern haurà de ser identificat pel personal de recepció.

Aquest accés autoritzat es podrà realitzar sota les següents condicions:

- Tenen accés a les diferents oficines de l'OPC per a l'exercici de la seva activitat exclusivament el personal intern de l'empresa. Aquesta autorització d'accés físic és atorgada a cada treballador en el moment de la signatura del contracte laboral, i és revocada i per tant anul·lada quan deixa de pertànyer a la plantilla de treballadors de l'empresa, no podent accedir més a les instal·lacions, tret que ho faci en règim de visita i amb la pertinent autorització del responsable dels Fitxers.
- Les terceres persones que en qualitat de visitant o de personal de serveis externs accedeixin a les oficines on l'OPC desenvolupa les seves activitats, han de comptar amb el beneplàcit del corresponent responsable.
- El personal que observi la presència de personal estrany a les oficines haurà de notificar-lo immediatament.
- Les pantalles de visualització de dades estan orientades en posicions que no permeten veure amb facilitat a tercers aliens a l'empresa el contingut d'aquestes.
- Els terminals informàtiques tenen una ubicació individualitzada per usuari, i el seu accés està controlat per un responsable, i només els usuaris autoritzats en l'annex 5 tenen accés.

2. Sistemes de seguretat física

Les mesures de seguretat necessàries per a impedir l'accessibilitat a les oficines de l'OPC així com les dels servidors on hi ha desat el fitxer de dades personals depenen directament de l'Ajuntament d'Olot. Totes aquestes mesures compleixen els requisits exigits per la Llei i, si escau, per les Ordenances Municipals vigents.

ANNEX 5 – AUTORITZACIONS D'ACCÉS ALS FITXERS I ZONES RESTRINGIDES

En aquest annex s'inclourà un detall de les persones (o unitats operatives, però preferiblement persones) que s'identifiquen com a responsables en els diferents nivells que estimi oportuns el responsable del fitxer com a conseqüència de la implantació efectiva del document de seguretat i la identificació i la assignació de funcions (la llista pot variar). Per a cada apartat s'inclourà una petita taula amb el format següent:

ADMINISTRADORS DELS FITXERS

Àrea	**Accessos**	**Restriccions**
Àrea tècnica de serveisweb		Modificació sense consentiment

ADMINISTRADORS DEL SISTEMA O PERSONAL INFORMÀTIC

Àrea	**Accessos**	**Restriccions**
Informàtica de l'Ajutnament d'Olot		Modificació sense consentiment

USUARIS DELS FITXERS

Nom i cognoms	**Àrea**	**Accessos**	**Restriccions**
Anna Montero	Àrea administrativa	Modificació, actualització i consulta	
Montse Vila	Àrea administrativa	Modificació, actualització i consulta	
Gemma Bretcha	Àrea tècnica	Consulta	
Anna Jiménez	Àrea tècnica	Modificació i consulta	

ANNEX 6 - PROCEDIMENTS DE SEGURETAT: SEGURETAT LÒGICA

1.- Sistema d'autenticació

1.1. Identificació
1. L'OPC ha establert un sistema d'identificació i autenticació inequívoc i personalitzat per als seus usuaris, com mesura de seguretat per a evitar accessos no autoritzats als sistemes informàtics que allotgen els Fitxers, i que contenen dades de caràcter personal.
2. Tot el personal de l'OPC amb accés autoritzat al sistema informàtic que conté els Fitxers, posseeix un nom d'usuari i una contrasenya com mesura d'identificació i autenticació.
3. Tots els usuaris del sistema informàtic de l'OPC són identificats en el moment de cursar-ne l'alta com a treballadors, mitjançant fotocòpia del DNI, passaport o targeta de residència.

1.2. Autenticació
1. A cada usuari del sistema se li assigna un identificador i una clau.

1.3. Assignació de contrasenyes
1. És competència dels administradors del sistema la assignació de les contrasenyes del personal intern de l'OPC.
3. L'assignació de contrasenyes es realitzarà de manera automàtica. L'usuari estarà obligat a modificar la seva contrasenya en el primer accés al sistema i haurà de modificar-la periòdicament quan el sistema li ho sol·liciti.
4. En cap cas l'administrador no està capacitat per a conèixer la contrasenya d'un usuari. En cas de pèrdua o d'oblit de la contrasenya, la contrasenya anterior quedarà anul·lada amb caràcter general i es subministrarà una nova contrasenya a l'usuari.

1.5. Emmagatzematge de contrasenyes
1. Els login i les claus d'accés assignades a cada usuari de l'OPC són personals i intransferibles, essent l'usuari l'únic responsable de les conseqüències que puguin derivar-se'n del mal ús, de la divulgació o de la pèrdua.
2. Durant el temps de vigència, les contrasenyes s'emmagatzemaran de forma inintel·ligible i seran salvaguardades en els processos de còpia de seguretat del sistema.
3. Ningú no està autoritzat a desxifrar la clau d'un usuari, ni tan sols el personal tècnic de suport. En cas de pèrdua o d'oblit per part de l'usuari, se li generarà una nova clau d'accés sotmesa als mateixos requisits que una clau inicial.

1.6. Característiques de les contrasenyes
1. Les contrasenyes d'accés són exclusivament conegudes per l'usuari propietari de les mateixes i pel responsable dels Fitxers o si escau l'administrador del sistema.
2. Els usuaris tenen l'obligació de tractar-les com informació confidencial, personal i intransferible. Cadascun els usuaris de l'OPC es responsabilitza d'assegurar la confidencialitat i custòdia de la seva contrasenya.
3. Des de l'àrea d'administradors del sistema s'han establert certes consideracions a l'hora de triar les contrasenyes:

Longitud mínima	6 caràcters que han d'incloure alguna majúscula i algun número o caràcter estrany
Canvi de contrasenyes	Automàtic cada 90 dies. Prohibició als usuaris de repetir l'última contrasenya
Responsable canvi	Administradors del sistema
Obligacions i Prohibicions	- S'evitaran noms comuns, nombres de matrícules, telèfons, noms de familiars, amics, etc., i derivats del nom de l'usuari com permutacions o canvi d'ordre de les lletres, transposicions, repeticions d'un únic caràcter, etc… - Els usuaris seran responsables també de la seva salvaguarda i custòdia.

ANNEX 7 – CÒPIES DE SEGURETAT I RECUPERACIÓ I GESTIÓ DE SUPORTS

A fi de complir allò que s'estableix en l'article 8.2.f del Real Decret 994/1999, de 11 de juny, l'àrea d'informàtica de l'Ajuntament d'Olot disposa d'un procediment de realització de còpies de seguretat i de recuperació de dades que en garanteix la reconstrucció en l'estat en què es trobaran en el moment de produir-se la pèrdua o la destrucció.

1.- Normes sobre còpies de seguretat i gestió de suports

En cas de produir-se una incidència que generi destrucció d'informació, s'aplicarà el procediment de notificació, de tractament i de registre d'incidències previst en el document de seguretat, i es procedirà a la recuperació de la informació destruïda. Si aquesta recuperació fos impossible, es procedirà a sol·licitar la còpia de seguretat més recent i a restaurar la informació destruïda.

2.- Procediments de còpia de seguretat i de recuperació de dades

D'acord amb les mesures de seguretat en matèria de còpia i de recuperació de dades establertes en aquest document i les especificacions manifestades pel responsable de fitxer i pel responsable del seu tractament, l'administrador de còpies mantindrà actualitzada la documentació sobre els procediments de còpia i de recuperació de dades per a cadascun dels servidors afectats i els fitxers que conté.

2.1. Sistema, Freqüència, Vigència i Històric de les còpies

Sempre que, en cas d'incidència es requereixi la recuperació de part o de la totalitat de les dades, sobretot pel que fa a fitxers protegits, s'aplicaran els procediments de recuperació preestablerts, quan la incidència sigui previsible, i els procediments que aconselli el Comitè de Crisi, quan la incidència obeeixi a una situació excepcional. En qualsevol cas, si es posen en perill fitxers protegits, serà necessària la conformitat per escrit del responsable de fitxer. Aquestes incidències quedaran enregistrades en el registre d'incidències.

Còpia a disc (Ajuntament d'Olot)

Suport de les còpies	Cintes LTO6
Sistema de còpies	Sistema BACKUP EXEC
Tipus de còpia	Automàtica assistida
Número de suports	1
Vigència / Històric	Còpies setmanals: 1 mes. Còpia mensual: 6 mesos. Còpia anual: 4 anys
Freqüència copia	Setmanalment
Responsable còpia	Administradors del sistema

Còpia a disc (Serveisweb)

Suport de les còpies	discs físics SATA, distribuïts en una matriu RAID10 + Host Spare
Sistema de còpies	Sistema Bacula Software
Tipus de còpia	Automàtica
Número de suports	1
Vigència / Històric	15 dies
Freqüència copia	Diaria. Una còpia sencera de totes les dades cada Dijous i sis còpies incrementals corresponents a la resta de dies de la Setmana
Responsable còpia	Administradors del sistema

Còpia a cinta (Ajuntament d'Olot)

Sistema de còpies	Aplicació VEEAM
Tipus de còpia	Automàtica
Número de suports	15 còpies sobre disc
Vigència / Històric	1 mes
Freqüència copia	Diàriament
Responsable còpia	Administradors del sistema

ANNEX 8 – FUNCIONS I OBLIGACIONS DEL PERSONAL

L'objectiu d'aquesta normativa és definir les responsabilitats del personal respecte a l'ús de la informació empresarial i dades personals responsabilitat de L'OPC, amb la finalitat de que tots els usuaris reconeguin i acceptin consensuadament les finalitats de la seva utilització i les seves limitacions.

Així mateix, la legislació vigent en relació a la Protecció de Dades Personals, obliga a l'OPC a complir amb una sèrie de requisits legals, entre els quals destaca l'obligació de posar en coneixement de tots els treballadors amb accés a dades personals, les seves funcions i obligacions en relació al tractament d'aquestes dades, especialment, en relació a les mesures de seguretat que s'han d'adoptar per a la seva custodia i protecció, que hauran de ser conegudes, acceptades i respectades per tot el personal amb accés al sistema informàtic de l'OPC, o qualsevol dels seus components, sobre la informació que conté o que ha estat elaborada per ell.

Classificació del personal
a) Responsable dels Fitxers
b) Usuaris dels Fitxers
c) Administradores del sistema o personal informàtic

FUNCIONS
a) Responsable del Fitxers

És el responsable jurídic de la seguretat dels seus Fitxers i l'encarregat d'establir les normes recollides en el present document, implantar les mesures de seguretat establertes en ell, i posar a disposició tots els mitjans necessaris perquè tots els usuaris afectats per aquest document, tinguin coneixement de totes les normes que afectin al desenvolupament de les seves funcions.

d) Usuaris del Fitxers

Els usuaris expressament autoritzats en el present document de seguretat s'encarreguen de les funcions de producció habitual i explotació diària de l'activitat de l'OPC. Sense perjudici que l'OPC pugui assignar funcions informàtiques a algun dels seus usuaris, aquests, en principi, no han de realitzar cap tipus activitat tècnic-informàtica.

e) Administradors del sistema o personal informàtic

Les funcions a ocupar pel personal informàtic o els administradors del sistema, es determinen en funció de la categoria informàtica que ostentin. Aquesta classificació, no significa que necessàriament hagin d'estar presents en tots els casos, sent en algunes ocasions assumides per una mateixa persona o persones.

A.- Obligacions que afecten al responsable dels fitxers
El responsable de fitxer, en coordinació amb els administradors del sistema, s'encarregarà de:

- Notificar a l'Agència de Protecció de Dades els fitxers amb dades personals existents a l'OPC, actualment i en el futur, com a conseqüència del desenvolupament de nous projectes o la implantació de nous serveis.
- Vetllar pel compliment de tots els requisits establerts a la Llei de Protecció de Dades de Caràcter Personal i al Reglament de Mesures de Seguretat dels Fitxers Automatitzats que continguin Dades de Caràcter Personal.
- Elaborar i implantar el Document de Seguretat i vetllar per la seva aplicació i el seu compliment.
- Descriure l'estructura dels fitxers i dels sistemes d'informació que realitzen el tractament de les dades personals de l'OPC.
- Definir els criteris que l'administrador de sistemes ha de seguir per tal d'administrar les autoritzacions d'accés a les dades i als recursos.
- Garantir la difusió d'aquest document entre tot el personal afectat.
- Mantenir actualitzat aquest document, sempre que es produeixin canvis rellevants en el sistema d'informació o en la seva organització, d'acord amb els articles 8 i 9 del Reglament.
- Vetllar per l'adequació en tot moment del document de seguretat a les disposicions vigents en matèria de seguretat de dades.
- Establir les funcions i les obligacions d'àmbit intern del personal al seu càrrec.

- Tramitar les sol·licituds d'accés als sistemes d'informació del seu personal, especificant els perfils d'usuari de cadascun partint de les seves funcions i la seva responsabilitat.
- Col·laborar en la redacció de les normes internes per als usuaris
- Publicar les normes internes
- Revisar la signatura de les normes internes per part del personal de l'OPC
- Vetllar pel compliment de les normes internes de l'OPC.

B.- Obligacions que afecten a tot el personal con accés a dades personals

1. Identificadors i claus d'accés

- És prohibit de comunicar a una altra persona l'identificador d'usuari i la clau d'accés. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i d'accés haurà de comunicar-ho al responsable de seguretat, per tal que li assigni una nova clau. Davant una baixa o absència temporal de l'usuari, el responsable del departament podrà sol·licitar al responsable de seguretat la cessió de la clau o dades a la persona designada per ell.
- L'usuari està obligat a complir tota la normativa relacionada amb els Identificadors i claus d'accés, i especialment, està prohibit la utilització de contrasenyes toves de fàcil identificació i amb menys de 6 caràcters, així com la repetició de l'última contrasenya quan el sistema li obligui al canvi de la mateixa.
- L'usuari està obligat a utilitzar la xarxa corporativa i la intranet de l'OPC i les seves dades sense incórrer en activitats que puguin ser considerades il·lícites o il·legals, que infringeixin els drets de l'OPC o de tercers, o que puguin atemptar contra la moral o les normes d'etiqueta de les xarxes telemàtiques.
- Estan expressament prohibides les activitats següents:
  - Compartir o facilitar l'identificador d'usuari i la clau d'accés donats per l'OPC amb una altra persona física o jurídica, inclòs el personal de la pròpia empresa. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable dels actes realitzats per la persona física o jurídica que utilitzi de forma no autoritzada l'identificador de l'usuari.
  - Intentar distorsionar o falsejar els registres LOG del sistema.
  - Intentar desxifrar les claus, sistemes o algorismes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de l'OPC.
  - Destruir, alterar, inutilitzar o de qualsevol forma danyar les dades, els programes o els documents electrònics de l'OPC o de tercers. (Aquests actes poden constituir un delicte de danys, previst a l'article 264.2 del Codi Penal).
  - Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris. (Aquesta activitat pot constituir un delicte d'intercepció de les telecomunicacions, previst a l'article 197 del Codi Penal).
  - Utilitzar el sistema per a intentar accedir a àrees restringides dels sistemes informàtics de l'OPC o de tercers.
  - Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics o qualsevol tipus d'obra o material els drets de propietat intel·lectual o industrial dels quals pertanyin a tercers, quan no s'hi disposi d'autorització.
  - Instal·lar o crear qualsevol programa, inclosos aquells que són estandarditzats, que impliqui tractament de dades personals, sense la deguda autorització del responsable dels fitxers o seguretat
  - Instal·lar còpies il·legals de qualsevol programa, inclosos aquells que són estandarditzats.
  - Esborrar qualsevol dels programes instal·lats legalment.
  - Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics de l'OPC, i també realitzar accions que perjudiquin, interrompin o generin errors en els sistemes esmentats.
  - Enviar missatges de correu electrònic de forma massiva o amb fins comercials o publicitaris sense el consentiment del destinatari (Spam).
  - Intentar augmentar el nivell de privilegis d'un usuari en el sistema.
  - Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin o siguin susceptibles de causar qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o de tercers. L'usuari tindrà l'obligació d'utilitzar els programes antivirus i les seves actualitzacions per a prevenir l'entrada en el sistema informàtic de qualsevol element a destruir o a corrompre les dades informàtiques.
  - Enviar o reenviar missatges en cadena o de tipus piramidal.

- L'enviament de missatges de correu electrònic on el remitent no estigui plenament identificat, o es presti confusió sobre la seva identitat.
- Variacions del contingut del correu electrònic i el seu enviament de forma maliciosa.

2.- Confidencialitat de la informació

- No es podran utilitzar els recursos del sistema d'informació als quals es tingui accés per a fins privades o per a qualsevol altra finalitat diferent de les estrictament relacionades amb la seva funció en l'empresa. Queda expressament prohibit la realització de còpies de cap tipus dels Fitxers per a ús privat en qualsevol tipus de suport.
- Està absolutament prohibit la comunicació de dades personals a tercers, excepte en els casos legalment prevists, i en aquells supòsits que sigui necessari per al desenvolupament de l'activitat laboral, sempre que aquestes comunicacions siguin legítimes.
- És prohibit d'enviar informació confidencial de l'OPC a l'exterior, mitjançant suports materials o per qualsevol mitjà de comunicació, incloent-hi la simple visualització o accés.
- Els usuaris dels sistemes d'informació corporatius hauran de guardar, per un temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni mitjançant terceres persones o empreses, les dades, els documents, les metodologies, les claus, les anàlisis, els programes i altra informació a la qual tinguin accés durant la seva relació laboral amb l'OPC, tant en suport material com electrònic. Aquesta obligació continuarà vigent un cop extingit el contracte laboral.
- Cap col·laborador no podrà posseir, per a usos que no siguin propis de la seva responsabilitat, cap material o informació propietat de l'OPC, tant ara com en el futur.
- En cas que, per motius directament relacionats amb el lloc de treball l'empleat prengui possessió d'informació confidencial sota qualsevol tipus de suport, s'entendrà aquesta possessió com estrictament temporal, amb obligació de secret, sense que aquest fet li concedeixi cap dret de possessió, o de titularitat o còpia sobre la informació esmentada. A més, el treballador haurà de tornar aquest materials a l'OPC, immediatament després de la fi de les tasques que n'han originat l'ús temporal i, en qualsevol cas, en acabar la relació laboral. La utilització continuada de la informació en qualsevol format o suport de manera diferent a aquella pactada i sense el coneixement de l'OPC no suposarà, en cap cas, una modificació d'aquesta clàusula.
- L'incompliment d'aquesta obligació pot constituir un delicte de revelació de secrets, previst a l'article 197 i articles següents del Codi Penal i donarà el dret a l'OPC d'exigir a l'usuari una indemnització econòmica.

3.- Ús del correu electrònic

- El sistema informàtic i els terminals utilitzats per tot usuari són propietat de l'OPC.
- En cas de conflicte, l'OPC es reserva el dret de revisar els missatges de correu electrònic dels usuaris de la xarxa corporativa i els arxius LOG del servidor, per tal de comprovar el compliment d'aquestes normes i de prevenir activitats que puguin afectar l'OPC com a responsable civil subsidiari. Aquesta revisió serà supervisada pel responsable de seguretat i es realitzarà sota el principi casuístic (cas a cas), sota el principi de bona fe (actuar amb preavís i en benefici del patrimoni empresarial) i sota el principi de garantia (respectant la dignitat del treballador).
- Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari mitjançant missatges de correu electrònic que provinguin de xarxes externes haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.

4.- Accés a Internet

- L'accés debat en temps real (Chat / IRC) és especialment perillós, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, per la qual cosa el seu ús és estrictament prohibit.
- En cas de conflicte, l'OPC es reserva el dret de monitoritzar i de comprovar, de forma aleatòria i sense avís previ, qualsevol sessió d'accés a Internet iniciada per un usuari de la xarxa corporativa
- Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari des d'Internet haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.
- La navegació per pàgines d'Internet inadequades o il·legals, no limitant-se exclusivament a les pornogràfiques, i la descarrega de qualsevol tipus de continguts que no siguin per a ús empresarial.

- La navegació per pàgines d'Internet en horari laboral que no tingui relació amb l'activitat desenvolupada.

5.- Propietat intel·lectual i industrial

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

6.- Incidències

- Tot el personal de l'OPC té l'obligació de comunicar qualsevol incidència que es produeixi en els sistemes d'informació als quals tingui accés.
- Entenem per incidència qualsevol anomalia que afecti o pugui afectar la seguretat de les dades i el seu correcte tractament, i també el correcte funcionament dels equips i dels programes per mitjà dels quals es realitza.
- Aquesta comunicació s'haurà de realitzar immediatament. Els responsables de cada grup operatiu seran informats del procediment i dels punts de suport als quals ha de dirigir-se tot usuari per notificar les incidències detectades en el compliment de les seves funcions i s'encarregaran de notificar-ho de manera fefaent a cadascun dels usuaris del grup.
- Qualsevol usuari que detecti una incidència és el responsable de comunicar-la pel procediment i al punt de suport que té assignat o, per defecte, al responsable de seguretat o al responsable del fitxer afectat, quan sigui el cas.
- El coneixement i la no notificació d'una incidència per part d'un usuari serà considerat com una falta contra la seguretat del sistema i, donat el cas, del fitxer afectat, per part d'aquest usuari.

7.- Protecció de dades

És terminantment prohibit de:

- Crear fitxers paral·lels o extreure parts dels fitxers de dades personals sense l'autorització del responsable del fitxer.
- Creuar informació relativa a dades de diferents fitxers o serveis a fi i efecte d'establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sens l'autorització expressa del responsable del fitxer.
- Tot el personal està obligat a atendre tota sol·licitud d'accés, rectificació i cancel·lació de dades personals sol·licitada per qualsevol persona, i ho posarà en coneixement del responsable de Fitxers.
- Qualsevol altra activitat expressament prohibida en aquest document o en les normes sobre protecció de dades i Instruccions de l'Agència de protecció de Dades.
- La manipulació i tractament d'imatges alienes a l'usuari de la Intrauoc i Campus Virtual.
- La recollida de dades personals sense el degut consentiment de l'afectat i sense informar-li de les obligacions exigides en l'article 5 de la Llei de Protecció de Dades.
- La contractació de serveis externs que impliquin comunicació de dades personals o accessos als mateixos, sense la deguda autorització i supervisió del responsable dels fitxers o responsable de protecció de dades.

Deure de secret:

- De conformitat amb l'art. 10 de la Llei 15/1999, de 13 de desembre de 1999 de Protecció de Dades de Caràcter Personal: el responsable del fitxer i aquells que intervinguin en qualsevol fase del tractament de les dades de caràcter personal n'estan obligats al secret professional i al deure de guardar-los. Aquestes obligacions encara subsistiran després de finalitzar les seves relacions laborals amb el titular del fitxer, o, donat el cas, amb el seu responsable.
- Tot el personal està obligat a posar en coneixement dels seus responsables qualsevol dubte que tingui sobre l'ús i tractament de les dades personals.

8.- Llocs de treball

- Un lloc de treball és responsabilitat de l'usuari al qual està assignat. L'usuari garantirà que se'n fa un ús apropiat i que la informació que mostra no és visible per al personal no autoritzat.
- Si per qualsevol motiu raonable un altre usuari ha de d'accedir al sistema des del lloc de l'usuari habitual, aquest segon usuari tancarà tots els recursos oberts i sortirà del sistema per forçar l'usuari ocasional a identificar-se amb el seu propi login d'accés i d'aquesta manera establir el seu perfil d'autoritzacions.

- Si un usuari autoritat ha de compartir impressores o altres perifèrics de sortida de dades amb usuaris no autoritzats, procurarà recollir immediatament els llistats, els documents, els informes, etc... de la seva competència.
- En qualsevol cas, l'usuari sol·licitant és el responsable de la destinació dels llistats, dels informes o de qualsevol altra informació de sortida sol·licitada. Per aquest motiu, no s'han de deixar documents sense recollir en les safates de sortida d'impressores o altres perifèrics.
- Quan l'usuari abandoni el seu lloc de treball, temporalment o en acabar la seva jornada laboral, haurà de deixar-lo apagat o bé bloquejat. Això últim es farà preferentment sortint l'usuari del sistema de manera manual; per defecte, s'activarà automàticament un protector de pantalla que obligui a identificar-se mitjançant la clau per poder reprendre la feina.
- En el cas que els tractaments de dades personals dutes a terme pels usuaris puguin ser visualitzats per persones no autoritzades, tant internes com externes, en la mesura del possible, haurien d'orientar les pantalles d'ordinador de manera que impedeixin la seva visualització.
- Els llocs de treball tenen una configuració determinada (sistema operatiu, aplicatius, software ofimàtic, antivirus, etc....) que només podrà ser modificada a petició del responsable del grup operatiu, sota la supervisió del responsable de seguretat i pel personal de suport degudament autoritzat.
- L'accés a fitxers protegits està configurat partint de les autoritzacions de l'usuari i controlat pels aplicatius i eines utilitzades. És prohibit de descarregar dades als discs locals del lloc de treball i és necessari mantenir qualsevol feina dins de les unitats de xarxa assignades, garantint-ne, d'aquesta manera, la seguretat i còpies dins dels procediments habituals del sistema.
- Està prohibit l'ús de dispositius informàtics mòbils com ordinadors portàtils o agendes electròniques que continguin dades de caràcter personal fora dels centres de treball, sense la deguda autorització per escrit del responsable dels fitxers o seguretat.

9.- Tractament de dades personals en suport paper

- No està permès llençar documents i papers que continguin dades personals, sense adoptar les mesures necessàries que impedeixin la seva posterior visualització, fins i tot en els recipients destinats a la deixalla del paper.
- No està permès la reutilització de documents i papers que continguin dades de caràcter personal.
- Tots els usuaris quan abandonin els seus llocs de treball, haurien de guardar convenientment la documentació que contingui dades personals, així com evitarà deixar documents damunt de les taules de treball.
- Quan per l'activitat desenvolupada es manipulin cartes, paquets, documents i similars en llocs d'accés al públic, s'haurien de prendre les mesures de seguretat oportunes per a evitar accessos no autoritzats als mateixos.
- Les mesures de seguretat descrites en aquest document i les funcions i les obligacions del personal seran d'igual aplicació quan l'accés es produeixi en la modalitat de teletreball i/o fora dels locals de l'organització.

C- Obligacions que afecten als administradors del sistema i personal informàtic

a) Administradors del sistemes

- Vigilar el compliment de les normes de seguretat establertes en aquest document de seguretat.
- Elaborar les mesures, les normes, els procediments, les regles i els estàndards de seguretat aplicats a l'OPC.
- Definir l'àmbit d'aplicació del document de seguretat.
- Decidir i documentar els recursos informàtics subjectes al document de seguretat.
- Definir i verificar l'aplicació dels procediments de gestió d'incidències.
- Definir i verificar l'aplicació dels procediments de còpies de seguretat i de recuperació de dades.
- Elaborar i mantenir actualitzat el registre d'usuaris amb accés als sistemes d'informació.
- Definir i verificar l'aplicació del procediment d'identificació i d'autenticació d'usuaris.
- Definir i verificar l'aplicació del procediment d'assignació, de distribució i d'emmagatzematge de contrasenyes.
- Definir i verificar l'aplicació del procediment de canvi periòdic de les contrasenyes dels usuaris.
- Definir i verificar el mètode aplicat per a l'emmagatzematge encriptat de les contrasenyes.

- Definir i verificar l'aplicació i l'efectivitat d'un sistema de control d'accessos que limiti l'accés dels usuaris únicament a aquelles dades i a aquells recursos que els siguin autoritzats per al desenvolupament de la seva activitat.
- Administrar les autoritzacions d'accés segons els criteris establerts pel responsable del fitxer.
- Definir i verificar la implantació d'un sistema de gestió de suports informàtics que contenen dades de caràcter general.
- Confirmar la sortida de suports informàtics que continguin dades de caràcter personal, prèvia autorització del responsable del fitxer.
- Verificar que es compleixen les normes de seguretat, informant el cap de personal de les infraccions comeses, per a l'aplicació de les sancions que se'n deriven.
- Coordinar i controlar les mesures definides en el document de seguretat amb el responsable del fitxer i els responsables de l'àrea de Sistemes d'Informació encarregats de l'administració de sistemes, del desenvolupament i del manteniment d'aplicatius, i de donar suport tècnic a la implantació efectiva de les mesures de seguretat descrites en aquest document.
- Controlar i coordinar les mesures definides en el document de seguretat amb el del fitxer i els responsables de les empreses proveïdores de serveis que actuen com a encarregats del tractament per compte l'OPC, i com a empreses de suport tècnic i outsourcing.

b) Personal Informàtic

Dins d'aquest col·lectiu es troben catalogats els professionals amb coneixements i amb capacitat per a actuar en els nivells més baixos de les capes de seguretat del sistema informàtic tant de l'àrea informàtica de l'Ajuntament d'Olot com de l'empresa Serveisweb. Per aquest motiu, el responsable de fitxers farà arribar el coneixement i la comprensió de les mesures de seguretat establertes en aquest document als responsables informàtics que correspongui.

Tot i que no tot el personal informàtic està afectat pel mateix nivell de responsabilitat ni d'autorització en el seu accés al sistema informàtic, sí que ha d'existir una consciència clara dels aspectes legals recollits a les normes a les quals hem estat fent referència, i també de la necessitat que el sistema informàtic de l'OPC gaudeixi d'una seguretat efectiva derivada d'una correcta aplicació de les tecnologies utilitzades i de la feina responsable de cadascun dels empleats en l'execució de les seves funcions.

El director de l'Àrea d'informàtica de l'Ajuntament d'Olot així com el responsable de l'empresa Serveisweb decidiran les persones que es responsabilitzaran en tot moment de les funcions de seguretat que es deriven de les normes establertes en aquest document i comunicarà les directrius que cal aplicar en l'execució de les seves funcions.

ANNEX 9 – PROCEDIMENT DE NOTIFICACIÓ I GESTIÓ D'INCIDÈNCIES

L'OPC registra les incidencia a l'àrea d'informàtica de l'Ajuntament d'Olot o a l'empesa Serveisweb depenent de si la incidència té lloc a nivel de xarxa local o a nivell d'internet. En el primer cas es fa mitjançant el correu incidencies@olot.cat. En el segon cas, es realitza la incidència mitjançant el panell d'administració del nostre servidor. En cada cas, és el proveïdor i no l'OPC l'encarregat de gestionar el registre d'incidències.