ATM Autoritat Territorial de la Mobilitat Camp de Tarragona

Consorci del Transport Públic del Camp de Tarragona. Autoritat Territorial de la Mobilitat

Document de Seguretat

xxx de xxxxxx del 2017

Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat
C. Anselm Clavé, 1 - 43004Tarragona · 977921956 · info@atmcamptarragona.cat

ATM Camp de Tarragona
Autoritat Territorial de la Mobilitat

Continguts

A. Objecte del document 3
B. Àmbit d'aplicació 3
1. Recursos protegits 3
2. Normativa aplicable 4
C. Funcions i obligacions del personal 4
D. Normes i procediments de seguretat 5
1. Mesures de seguretat aplicables a tots els fitxers 5
1.1. Centres de tractament i locals 5
1.2. Llocs de treball 5
1.3. Entorn de Sistema Operatiu i Comunicacions 7
1.4. Sistema Informàtic o aplicacions d'accés als fitxers 7
1.5. Gestió d'usuaris 8
1.6. Gestió de suports i documents 9
1.7. Gestió d'incidències 10
1.8. Procediment de còpies de seguretat i recuperació de dades 10
2. Mesures de seguretat aplicables als fitxers de nivell mitjà i alt 11
2.1. Responsable de seguretat 11
2.2. Fitxers no automatitzats 11
2.3. Gestió de suports 12
2.4. Procediment de còpies de seguretat i recuperació de dades 12
2.5. Entrada i sortida de dades a través de la xarxa 12
2.6. Controls periòdics de verificació del compliment 13

A.Objecte del document

El present document respon a l'obligació establerta a l'article 88 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de caràcter personal (en endavant, RLOPD).

Per tant, són aplicables a aquests les mesures de seguretat que s'estableixen als Capítols III i IV del Títol VIII del citat decret, en funció del seu nivell de dades.

B.Àmbit d'aplicació

Aquest document ha estat elaborat sota la responsabilitat de l'ATM del Camp de Tarragona, qui, com a responsable del fitxer, es compromet a implantar i actualitzar aquesta Normativa de Seguretat d'obligat compliment per a tot el personal amb accés a les dades protegides o als sistemes d'informació que permeten l'accés a aquestes.

Totes les persones que tinguin accés a les dades dels fitxers, amb independència del sistema de tractament utilitzat (informatitzat, manual o mixt), es troben obligades, per llei, a complir el que s'estableix en aquest document, quedant subjectes a les conseqüències en què poguessin incórrer en cas d'incompliment.

Una còpia d'aquest document, amb els aspectes que els hi siguin directament d'aplicació, serà lliurada, per al seu coneixement, a cada persona autoritzada a accedir a les dades dels fitxers, essent requisit obligatori per poder tenir accés a aquestes dades haver signat la recepció del mateix.

1. Recursos protegits

La protecció de les dades dels fitxers, davant accessos no autoritzats, s'haurà de realitzar mitjançant el control de totes les vies per les quals es pugui tenir accés a aquesta informació.

Els recursos que, pel fet de servir com a mitjà directe o indirecte per accedir als fitxers, hauran d'ésser controlats per aquesta normativa són:

- Els sistemes informàtics o aplicacions establertes per accedir a les dades, els quals es descriuen a l'annex C del document Annexos del Document de Seguretat.
- Els servidors, en cas que hi haguessin, i l'entorn del sistema operatiu i de comunicacions als que es trobin ubicats els fitxers. Aquests estan descrits a l'annex D del document Annexos del Document de Seguretat.
- Els centres de tractament i locals on es troben ubicats els fitxers o s'emmagatzemen els suports que els continguin. La seva descripció figura a l'annex E del document Annexos del Document de Seguretat.

- Els llocs de treball, locals o remots, des dels quals es pugui tenir accés als fitxers. La relació dels llocs de treball es troba descrita a l'annex E del document Annexos del Document de Seguretat.

2. Normativa aplicable

La legislació utilitzada per a la realització d'aquest document és la següent:

- La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de caràcter personal (LOPD).
- Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de caràcter personal (RLOPD).
- Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades.
- Instrucció 1/2009, de 10 de febrer, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.

C. Funcions i obligacions del personal

El personal afectat per aquesta normativa es classifica en dues categories:

- Administradors del sistema. Són els encarregats d'administrar o mantenir l'entorn operatiu dels fitxers, ja que, per les seves funcions, poden utilitzar eines d'administració que permetin l'accés a les dades protegides passant-se per alt les barreres d'accés a l'aplicació o fitxer. Aquest personal haurà d'estar explícitament relacionat a l'annex F.
- Usuaris dels fitxers. És el personal que habitualment utilitza els fitxers i que té accés al sistema informàtic d'accés als fitxers, els quals estan degudament relacionats a l'aplicació informàtica confeccionada a tal efecte tant per a l'administració com per a la gestió de permisos i perfils d'usuari.

A més del personal anteriorment citat, existeix un responsable de seguretat que té la funció de coordinar i controlar les mesures definides en aquest document, servint al mateix temps d'enllaç amb el responsable del fitxer sense que això suposi, en cap cas, una delegació de la responsabilitat que correspon a aquest últim, d'acord amb allò que estableix l'article 84 del RLOPD.

A més a més, si existeix un encarregat del tractament (administrador o usuari) que sigui una empresa externa o tercer diferent al responsable del fitxer, haurà d'estar relacionat a l'annex J.

Aquest document és d'obligat compliment per a tots ells. Les funcions i obligacions del personal venen descrites a l'annex H del document Annexos del Document de Seguretat. No obstant això, els administradors del sistema hauran d'atenir-se també a aquelles normes més extenses i estrictes que es troben referenciades a l'annex G del citat document. Aquestes normes es refereixen, entre d'altres, al tractament de les còpies de seguretat, a l'alta dels usuaris i a les paraules de pas, recollint també altres normes d'obligat compliment per a la unitat administrativa o departament al que pertanyin els fitxers.

D. Normes i procediments de seguretat

1. Mesures de seguretat aplicables a tots els fitxers

1.1. Centres de tractament i locals

Els locals on s'ubiquin els fitxers, i els equips que donen suport als sistemes d'informació que contenen els fitxers, han de ser objecte d'especial protecció, de manera que es garanteixi la disponibilitat i confidencialitat de les dades protegides, especialment en el cas de què els fitxers s'ubiquin en un servidor accedit mitjançant una xarxa.

Els locals hauran de comptar amb els mitjans mínims de seguretat que evitin els riscos d'indisponiblitat dels fitxers que puguin produir-se com a conseqüència d'incidències fortuïtes o intencionades i controlar l'accés a la informació, de forma que només estigui permès a les persones autoritzades a tal efecte pels Caps de Servei en atenció a les seves competències. La descripció d'aquests locals i equipaments es troba a l'annex E del document Annexos del Document de Seguretat.

L'accés als locals on es trobin els fitxers haurà d'estar controlat i, en la cas de la Sala de servidors, restringit exclusivament als administradors del sistema que hagin de realitzar tasques de manteniment per les quals sigui imprescindible l'accés físic.

1.2. Llocs de treball

Són tots aquells llocs de treball de les persones que treballen al servei de l'ATM del Camp de Tarragona, els quals disposen de 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 fitxers.

Cada lloc de treball estarà sota la responsabilitat d'una de les persones autoritzades a l'annex F del document Annexos del Document de Seguretat, la qual garantirà que la informació disponible no pugui ser vista per persones no autoritzades.

Aquest fet implica que, tant les pantalles com les impressores o altres tipus de dispositius connectats al lloc de treball, hauran d'estar físicament ubicats a llocs que garanteixin aquesta confidencialitat.

La persona responsable de cada lloc de treball, en el cas de les impressores, haurà d'assegurar-se que no quedin documents impresos a la safata de sortida que continguin dades protegides. Si les impressores són compartides amb altres usuaris, i aquests no estan autoritzats per accedir a les dades dels fitxers, els responsables de cada lloc de treball hauran de retirar els documents conforme es vagin imprimint.

- Quant als fitxers no automatitzats:

Cada lloc de treball és responsable de la custòdia dels documents amb els que estigui treballant durant la jornada laboral, havent de controlar que persones no autoritzades no puguin accedir-hi, en el cas que aquests no estiguin ubicats en armaris.

En finalitzar la jornada, cada lloc de treball ha d'assegurar-se que els documents que continguin dades de caràcter personal estiguin en armaris tancats amb clau o en alguna ubicació que impedeixi l'accés a persones no autoritzades.

A més, els documents s'arxivaran seguint els criteris previstos per l'organització, o per la legislació específica que els hi aplica, havent de garantir en tot moment la seva correcta conservació i la seva localització i consulta, així com permetre l'exercici dels drets per part dels usuaris.

Cal establir un procediment per al trasllat de la documentació a l'Arxiu, garantint la seva localització i conservació.

- Per als fitxers automatitzats:

Quan el responsable d'un lloc de treball l'abandoni, bé temporalment o bé al finalitzar el seu torn de treball, haurà de deixar-lo en un estat que impedeixi la visualització de les dades protegides. Això es podrà realitzar mitjançant un protector de pantalla amb paraula de pas. D'aquesta manera, per reprendre el treball s'haurà de desactivar la pantalla protectora amb la introducció de la paraula de pas corresponent.

En el cas d'accessos a xarxes o sistemes remots mitjançant els quals es realitzin accessos als fitxers, aquests es faran per mitjà dels protocols d'encriptació i seguretat de comunicacions establerts a la xarxa corporativa. En aquest sentit, queda expressament prohibida la connexió a xarxes o sistemes exteriors dels llocs de treball des dels quals es realitza l'accés als fitxers. La revocació d'aquesta prohibició haurà de ser autoritzada pel responsables del fitxer, deixant constància d'aquesta modificació al Registre d'Incidències.

Els llocs de treball des dels quals es té accés als fitxers tindran una configuració fixa a les seves aplicacions i sistemes operatius que sols podrà ser canviada sota autorització del responsable de seguretat o pels administradors autoritzats a l'annex F del document Annexos del Document de Seguretat.

1.3. Entorn de Sistema Operatiu i Comunicacions

Donat que els fitxers es troben en una xarxa interconnectada que permet la comunicació amb d'altres ordinadors, seria possible, per a les persones que coneguin aquests entorns, accedir a les dades protegides eludint els procediments de control d'accés amb els que pugui comptar l'aplicació.

Aquesta normativa, per tant, ha de regular l'ús i accés de les parts del sistema operatiu, eines o programes d'utilitat, o de l'entorn de comunicacions, de manera 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 un responsable que, com a administrador, haurà d'estar relacionat a l'annex F del document Annexos del Document de Seguretat.

La creació d'un fitxer en l'àmbit local suposarà la total assumpció de responsabilitat, per part de l'usuari final, davant la implantació i el control de les mesures tècniques i controls de seguretat establerts per la legalitat vigent en aquesta matèria. En cas que el fitxer es trobi ubicat a un ordinador personal i accedit mitjançant una aplicació local, l'administrador del sistema operatiu podrà ser el mateix usuari que accedeix habitualment al fitxer.

Cap eina o programa d'utilitat que permeti l'accés als fitxers haurà de ser accessible a cap usuari o administrador no autoritzat a l'Annex F del document Annexos del Document de Seguretat o a l'aplicació corporativa de gestió d'usuaris.

A la norma anterior s'inclou qualsevol mitjà d'accés en brut, és a dir, no elaborat o editat, a les dades dels fitxers, com les anomenades *queries*, editors universals, analitzadors de fitxers, etc., que hauran d'estar sota el control dels administradors autoritzats relacionats a l'Annex F del document Annexos del Document de Seguretat.

L'administrador s'haurà de responsabilitzar de guardar en lloc protegit les còpies de seguretat dels fitxers, de manera que cap persona no autoritzada tingui accés a les mateixes.

Si l'aplicació o sistema d'accés als fitxers utilitzés usualment fitxers temporals, fitxers de logging o qualsevol altre mitjà en el qual poguessin ser gravades còpies de les dades protegides, l'administrador hauria d'assegurar-se que aquestes dades no són accessibles posteriorment per personal no autoritzat.

Si l'ordinador en el qual estan situats els fitxers està integrat en una xarxa de comunicacions de manera que, des d'altres ordinadors connectats a la mateixa, sigui possible l'accés als fitxers, l'administrador responsable del sistema haurà d'assegurar-se que aquest accés no es permet a persones no autoritzades.

1.4. Sistema Informàtic o aplicacions d'accés als fitxers

Són tots aquells sistemes informàtics, programes o aplicacions amb les quals es pot accedir a les dades dels fitxers, i que són usualment utilitzats pels usuaris per accedir a ells.

Aquests sistemes poden ser aplicacions informàtiques expressament dissenyades per accedir als fitxers o sistemes pre-programats d'ús general com aplicacions o paquets disponibles en el mercat informàtic.

Els sistemes informàtics d'accés als fitxers hauran de tenir el seu accés restringit mitjançant un codi d'usuari i una paraula de pas.

Tots els usuaris autoritzats per accedir als fitxers, relacionats a l'annex F del document Annexos del Document de Seguretat, hauran de tenir un codi d'usuari que serà únic i que estarà associat a la paraula de pas corresponent, que només serà coneguda pel propi usuari.

El responsable del fitxer vetllarà perquè els usuaris només puguin accedir a aquells recursos que necessiten per al desenvolupament de la seva feina i que han estat autoritzats per les persones responsables d'aquests.

Si l'aplicació informàtica que permet l'accés als fitxers no compta amb un control d'accés, haurà de ser el sistema operatiu on s'executa aquesta aplicació el que impedeixi l'accés no autoritzat, mitjançant el control dels anomenats codis d'usuari i paraules de pas.

En qualsevol cas, es controlaran els intents d'accés fraudulent al fitxer, limitant el nombre màxim d'intents fallits i, quan sigui tècnicament possible, guardant en un fitxer auxiliar la data, hora, codi i clau errònies que s'han introduït, així com d'altres dades rellevants que ajudin a descobrir l'autor dels intents d'accés fraudulents.

Si durant les proves anteriors a la implantació o modificació de l'aplicació d'accés als fitxers s'utilitzessin dades reals, s'haurà d'aplicar a aquests fitxers de prova el mateix tractament de seguretat que s'aplica al mateix fitxer, s'haurà de fer prèviament una còpia de seguretat del fitxer i s'hauran de relacionar aquests fitxers de prova a l'annex B del document Annexos del Document de Seguretat.

De cada intent d'accés es guardaran com a mínim, la identificació de l'usuari, la data i hora en què es va fer, el fitxer accedit, el tipus d'accés i si ha estat autoritzat o denegat. Si es tracta d'un accés autoritzat es guardarà la informació que permeti identificar el registre accedit.

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

En el cas de què personal aliè a l'organització tingui accés als fitxers, aquest haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal intern.

1.5. Gestió d'usuaris

Les paraules de pas personals constitueixen un dels components bàsics de la seguretat de les dades i, per tant, hauran d'estar especialment protegides. Com a claus d'accés al sistema, les paraules de pas hauran de ser estrictament confidencials i personals i qualsevol incidència que comprometi la seva confidencialitat haurà de ser immediatament comunicada a l'administrador i solucionada en el menor termini de temps possible.

Només les persones relacionades a l'Annex F podran tenir accés a les dades del fitxer.

Cada usuari serà responsable de la confidencialitat de la seva paraula de pas i, en cas que la mateixa sigui coneguda fortuïta o fraudulentament per persones no autoritzades, s'haurà de registrar com a incidència i procedir immediatament al seu canvi.

Les paraules de pas s'assignaran i es canviaran mitjançant el mecanisme i periodicitat que es determinen a l'Annex G del document Annexos del Document de Seguretat.

L'arxiu on s'emmagatzemin les paraules de pas haurà d'estar protegit i sota la responsabilitat de l'administrador del sistema, emmagatzemant-les, a més, de manera inintel·ligible.

1.6. Gestió de suports i documents

Suport és qualsevol objecte físic que emmagatzema o conté dades o documents, o objecte susceptible d'ésser tractat en un sistema d'informació i sobre el qual es poden gravar i recuperar dades.

Suports informàtics són tots aquells mitjans d'enregistrament i recuperació de dades que s'utilitzen per realitzar còpies o passos intermedis en els processos de les aplicacions que gestionen els fitxers.

Donat que la major part dels suports que avui en dia s'utilitzen, com disquets, CD-ROM, CD o memòries USB, són fàcilment transportables, reproduïbles o copiables, és evident la importància que per a la seguretat de les dades dels fitxers té el control d'aquests dispositius.

Els suports que continguin dades dels fitxers, sigui a conseqüència d'operacions intermèdies pròpies de l'aplicació que els tracta o bé com a conseqüència de processos periòdics de còpies de seguretat o de qualsevol altra operació esporàdica, hauran d'estar identificats amb una etiqueta externa que permeti conèixer quin és el seu contingut als usuaris autoritzats i que, a les persones no autoritzades, els dificulti saber el que contenen.

Aquells dispositius que siguin reutilitzables i que hagin contingut còpies de dades dels fitxers, hauran de ser buidats físicament abans de la seva reutilització, de manera que les dades que contenien no siguin recuperables.

De la mateixa manera, abans d'eliminar-ne un suport o document que contingui dades personals es destruirà o s'esborraran les dades que aquest conté, de forma que s'eviti l'accés de persones no autoritzades o la seva recuperació posterior.

Els suports que continguin dades dels fitxers hauran de ser emmagatzemats en llocs als quals no tinguin accés persones no autoritzades per a l'ús dels mateixos que no estiguin relacionades a l'Annex F del document Annexos del Document de Seguretat.

La sortida de suports o documents que continguin dades dels fitxers fora dels locals on es troben ubicats aquests, el que inclou els enviaments per correu electrònic, haurà de ser expressament autoritzada pel responsables del fitxer o estar autoritzada al Document de Seguretat. Utilitzant per a aquesta finalitat el document adjunt a l'annex G del document Annexos del Document de Seguretat.

El responsable del fitxer habilitarà un Registre d'entrades i sortides de suports, on es guardaran els formularis d'entrades i sortides dels suports descrits a l'annex G del document Annexos del Document de Seguretat, amb indicació del tipus de suport, data i hora, emissor/destinatari, nombre de suports, tipus d'informació que contenen, forma d'enviament i persona responsable del lliurament o de la recepció que haurà d'estar degudament autoritzada.

Quan els suports hagin de sortir fora dels locals en què es troben ubicats els fitxers, s'adoptaran les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada en ells.

1.7. Gestió d'incidències

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

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

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

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

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

La notificació o registre d'una incidència haurà de constar, com a mínim, de les següents dades: tipus d'incidència, data i hora en què es va produir o detectar, persona que realitza la notificació, persona a qui es comunica, efectes que poden derivar-se i mesures correctores aplicades. El procediment està descrit a l'Annex I del document Annexos del Document de Seguretat.

1.8. Procediment de còpies de seguretat i recuperació de dades

La seguretat de les dades personals dels fitxers no només suposa la confidencialitat dels mateixos sinó que també comporta la integritat i la disponibilitat d'aquestes dades.

Per garantir aquests dos aspectes fonamentals de la seguretat és necessari que existeixin uns processos de còpies de seguretat i de recuperació de les dades que, en cas de fallada del sistema informàtic, permetin recuperar i, si escau, reconstruir les dades dels fitxers.

Existirà una persona, sigui l'administrador o un altre usuari expressament designat, que serà la responsable d'obtenir periòdicament una còpia de seguretat dels fitxers a efectes de recolzament i possible recuperació en cas de fallada.

Aquestes còpies hauran de realitzar-se amb una periodicitat mínima setmanal, excepte en el cas de què no s'hagi produït cap actualització de les dades.

En cas de fallada del sistema amb pèrdua total o parcial de les dades dels fitxers existirà un procediment, informàtic o manual, que, partint de l'ultima còpia de seguretat i del registre de les operacions realitzades des del moment de la còpia, reconstrueixi les dades dels fitxers a l'estat en què es trobaven en el moment de la fallada. Aquest procediment està descrit a l'Annex G del document Annexos del Document de Seguretat.

Tan sols en aquells casos en els que els fitxers estiguin automatitzats, com a mínim en una part, i sigui possible reconstruir-los, amb els procediments de recuperació, després d'una pèrdua d'informació es gravaran dades manualment, fent constar al Document de Seguretat aquest fet.

El responsables del fitxer haurà de dur a terme operacions que li permetin verificar semestralment el correcte funcionament dels procediments establerts per a la realització de còpies i recuperació de dades.

2. Mesures de seguretat aplicables als fitxers de nivell mitjà i alt

2.1. Responsable de seguretat

El responsable de seguretat és la persona nomenada a l'annex F del document Annexos del Document de Seguretat.

El responsable de seguretat és l'encarregat de controlar i verificar els procediments de seguretat aplicables als sistemes d'informació i als tractament de dades, a nivell tècnic i organitzatiu de l'organització.

En cap cas, la designació del responsable de seguretat, suposarà una exoneració de les responsabilitats que corresponen al responsables del fitxer.

2.2. Fitxers no automatitzats

La documentació estarà ubicada en armaris tancats amb clau o mecanismes similars i, a la vegada, aquests s'ubicaran en zones d'accés restringit i protegit amb portes dotades d'un sistema d'obertura mitjançant una clau o un altre sistema anàleg, les quals romandran tancades sempre que no s'hagi d'accedir a les mateixes.

En cas que no sigui possible ubicar la informació en àrees d'accés restringit, donades les característiques dels edificis corporatius, caldrà prendre mesures alternatives, deixant constància d'aquest fet i de les mesures aplicades al Document de Seguretat.

En el cas dels fitxers automatitzats, també es limitaran els accessos a aquelles persones que hagin estat autoritzades a tal efecte a l'annex F, establint mecanismes per identificar els accessos realitzats i registrant de forma específica els accessos per part de persones que no estiguin autoritzades a l'annex esmentat.

Es limitarà la realització de còpies o la reproducció de les dades dels fitxers, el que només podrà fer-se sota la responsabilitat del personal autoritzat l'annex F. Tot i així, un cop es compleixi la finalitat per a la qual es va fer una còpia de la informació, aquesta serà destruïda de forma que no permeti l'accés a les dades que hi contenia o la reva recuperació posterior.

En el cas que es produeixin trasllats de documentació, caldrà prendre mesures per tal de garantir la seguretat de les dades durant aquest procés, evitant un possible accés o manipulació per persones no autoritzades.

2.3. Gestió de suports

La distribució dels suports que continguin dades de caràcter personal de nivell alt es realitzarà xifrant les dades o utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel·ligible ni manipulada durant el seu transport, així mateix es xifrarà el contingut de tots els dispositius portàtils que hagin de sortir de les instal·lacions. En el cas que els dispositius portàtils no permetin el xifrat, s'evitarà utilitzar aquests suport i si no es pot fer s'adoptaran altres mesures i s'indicaran als l'annex G dels Annexos del Document de Seguretat.

2.4. Procediment de còpies de seguretat i recuperació de dades

Serà necessària l'autorització per escrit del responsables del fitxer per a l'execució dels procediments de recuperació de dades i s'haurà de deixar constància, al Registre d'incidències, dels procediments realitzats de recuperacions de dades, incloent la persona que va realitzar el procés, les dades restaurades i, si s'escau, les dades que s'hagin hagut de gravar manualment en el procés de recuperació.

Haurà conservar-se una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent d'aquell en què es trobin els equips informàtics que les tracten complint, en tot cas, les mesures de seguretat exigides al RLOPD.

2.5. Entrada i sortida de dades a través de la xarxa

La transmissió de dades per xarxa, sigui via correu electrònic o amb sistemes de transferència de fitxers, s'està convertint en un dels mitjans més utilitzats per a l'enviament de dades, fins al punt que està substituint als suports físics. És per això que mereixen un tractament especial, ja que, per les seves característiques, poden ser més vulnerables que els suports físics tradicionals.

Totes les entrades i sortides de dades dels fitxers que s'efectuïn mitjançant correu electrònic es realitzaran des d'un únic compte o adreça de correu controlada per un usuari especialment autoritzat pel responsables del fitxer. Igualment, si es realitza l'entrada o sortida de dades mitjançant sistemes de transferència de fitxers per xarxa, únicament un usuari o administrador estarà autoritzat per realitzar aquestes operacions.

Es guardaran còpies de tots els correus electrònics que involucrin entrades o sortides de dades dels fitxers en directoris protegits i sota el control del responsable citat. Es mantindran còpies d'aquests correus durant un termini mínim de 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 la destinació del fitxer enviat.

Quan les dades dels fitxers s'enviïn per correu electrònic o per sistemes de transferència de fitxers, a través de xarxes públiques o no protegides, es recomana que aquests enviaments siguin encriptats, de manera que només puguin ser llegits i interpretats pel destinatari.

La transmissió de dades de caràcter personal mitjançant xarxes de telecomunicacions electròniques es realitzarà xifrant aquestes dades o bé utilitzant mecanismes que garanteixin que la informació no sigui intel·ligible ni manipulada per tercers.

2.6. Controls periòdics de verificació del compliment

La veracitat de les dades que contenen els annexos d'aquest document, així com el compliment de les normes que conté hauran de ser periòdicament comprovats, de manera que puguin detectar-se i corregir-se anomalies.

El responsable de seguretat comprovarà, amb una periodicitat mínima trimestral, que la llista d'usuaris autoritzats a l'Annex F del document Annexos del Document de Seguretat es correspon amb la llista dels usuaris realment autoritzats per accedir a l'aplicació d'accés als fitxers, per al que demanarà la llista d'usuaris i els seus codis d'accés a l'administrador o administradors dels fitxers. A més d'aquestes comprovacions periòdiques, l'administrador comunicarà al responsable de seguretat, qualsevol alta o baixa d'usuaris amb accés autoritzat als fitxers en el moment en què aquesta es produeixi.

Es comprovarà també, amb una periodicitat mínima trimestral, l'existència de còpies de seguretat que permetin la recuperació dels fitxers segons el que està estipulat a l'apartat B.2.4 d'aquest document.

De la mateixa manera, i també amb una periodicitat mínima trimestral, els administradors dels fitxers comunicaran al responsable de seguretat qualsevol canvi que s'hagi realitzat en les dades tècniques recollides als annexos d'aquest document, com, per exemple, canvis en el programari o maquinari, bases de dades o aplicacions d'accés als fitxers, procedint igualment a l'actualització d'aquests annexos.

El responsable de seguretat verificarà, amb una periodicitat mínima trimestral, el compliment del previst al apartat 2.3en relació amb les entrades i sortides de dades d'aquest document, siguin per xarxa o en suport magnètic.

El responsables del fitxer, juntament amb el responsable de seguretat, analitzarà, amb una periodicitat mínima trimestral, les incidències registrades per adoptar les mesures correctores que limitin aquestes incidències en el futur, independentment de les mesures particulars que s'hagin adoptat en el moment en què es van produir.

Cada dos anys, com a mínim, es realitzarà una auditoria, externa o interna, que dictamini el correcte compliment i l'adequació de les mesures del present Document de Seguretat a les exigències de la LOPD i del RLOPD, identificant les deficiències i proposant les mesures correctores necessàries. Aquest període pot ser menor en el cas que es produeixin canvis al sistema d'informació que puguin afectar a la implantació de les mesures de seguretat. Els informes d'auditoria seran analitzats pel responsable de seguretat, qui proposarà al responsables dels fitxer les mesures correctores corresponents.

Els mecanismes que permeten el registre d'accessos estaran sota el control directe del responsable de seguretat, sense que es permeti, en cap cas, la desactivació dels mateixos.

Els resultats de tots aquests controls periòdics, així com els de les auditories, seran adjuntats a l'annex K del document Annexos del document de Seguretat.

El responsable de seguretat s'encarregarà de revisar mensualment la informació de control registrada respecte dels accessos i elaborarà un informe de les revisions realitzades i dels problemes detectats.

Consorci del Transport Públic del Camp de Tarragona. Autoritat Territorial de la Mobilitat

Annexos Document de Seguretat

xx de xxxxxx del 2017

Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat
C. Anselm Clavé, 1 - 43004 Tarragona · 977 921 956 · info@atmcamptarragona.cat

ATM Camp de Tarragona
Autoritat Territorial de la Mobilitat

Continguts

A. ANNEX A. Documents de notificació i decrets 4
1. Ordre de declaració dels fitxers a l'APDCAT 4
B. ANNEX B. Descripció detallada de l'estructura dels fitxers o tractament 5
C. ANNEX C. Descripció del sistema informàtic d'accés al fitxer 17
D. ANNEX D. Entorn de sistema operatiu i de comunicacions del fitxer 18
1. Sistema Operatiu 18
2. Entorn de comunicacions 18
3. Representació gràfica de la xarxa corporativa 19
E. ANNEX E. Locals i equipament 20
1. Locals d'ubicació dels equips que donen suport als sistemes d'informació 20
2. Arxiu Documental 20
3. Equipament 20
F. ANNEX F. Personal autoritzat per accedir al fitxer 21
1. Responsable del tractament 21
2. Responsable de seguretat 21
3. Responsables de la gestió dels tractament que es duen a terme a cada Servei 21
4. Administradors de sistemes i de bases de dades i manteniment dels sistemes i aplicacions 21
G. ANNEX G. Procediments de control d'accés, suport, recuperació i gestió 22
1. Procediment d'assignació i canvi de paraules de pas 22
2. Procediment de còpies de seguretat i recuperació de dades 22
3. Procediment de gestió de suports 22
H. ANNEX H. Funcions i obligacions del personal 24
1. Funcions del responsable del fitxer 24
2. Funcions del responsable de seguretat 24
3. Classificació del personal d'administració o personal informàtic 24
4. Personal autoritzat en producció habitual 24
5. Administradors tècnics i informàtics generals que intervenen en situacions no habituals 24
6. Funcions dels administradors o personal informàtic 25
7. Obligacions del responsable del fitxer 25

7.1. Entorn de Sistema Operatiu i de Comunicacions 26
7.2. Sistema Informàtic o aplicacions d'accés al fitxer 26
7.3. Salvaguarda i protecció de les paraules de pas personals 26
7.4. Gestió de suports 26
7.5. Entrada i sortida de dades per xarxa 26
7.6. Procediments de recolzament i recuperació 26
7.7. Controls periòdics de verificació del compliment 27
8. Obligacions del responsable de seguretat 27
8.1. Gestió d'incidències 27
8.2. Controls periòdics de verificació del compliment 27
9. Obligacions que afecten a tot el personal 29
9.1. Llocs de treball 29
9.2. Salvaguarda i protecció de les paraules de pas personals 29
9.3. Gestió d'incidències 29
9.4. Gestió de suports 30
10. Obligacions dels administradors i personal informàtic 30
10.1. Entorno de sistema operatiu i de comunicacions 30
10.2. Sistema Informàtic o aplicacions d'accés al fitxer 31
10.3. Salvaguarda i protecció de les paraules de pas personals 31
10.4. Procediments de recolzament i recuperació 32
10.5. Controls periòdics de verificació del compliment 32
I. ANNEX I. Procediment de notificació i gestió d'incidències 34
J. ANNEX J. Relació de contractes amb tercers amb accés als fitxers 35
1. Relació dels tercers que tracten les dades a les instal·lacions de l'ATM 35
2. Relació dels tercers que accedeixen als sistemes d'informació de l'ATM amb accés remot 36
3. Relació dels tercers que tracten les dades a les seves instal·lacions 37
K. ANNEX K. Controls periòdics i auditories 38
1. Relació d'actualitzacions 38
2. Auditories realitzades 38

A. ANNEX A. Documents de notificació i decrets

A continuació es detallen el codi d'inscripció, el nom i la descripció dels fitxers que consten inscrits al Registre General de Protecció de Dades de Catalunya de l'Autoritat Catalana de Protecció de Dades[1].

1. Ordre de declaració dels fitxers a l'APDCAT

Núm. d'inscripció:	
Nom fitxers inscrits:	– Persones usuàries – Contractació – Registre d'entrada i sortida – Membres dels òrgans estatutaris – Suggeriments, reclamacions i consultes – Contactes – Recursos humans – Accions promocionals

[1] El detall de la informació relativa als fitxers està continguda a les fitxes de notificació dels fitxers que s'annexen a aquest apartati que van ser enviades a l'Autoritat Catalana de Protecció de Dades.

B. ANNEX B. Descripció detallada de l'estructura dels fitxers o tractament

1.Denominació: **Persones usuàries**

a)Finalitat i usos previstos:

La finalitat del fitxer és la gestió de les targetes de transport del sistema tarifari integrat de l'ATM del Camp de Tarragona.

Els usos del fitxer són emetre targetes de transport personalitzades i atendre'n les incidències com ara el seu bescanvi o substitució i la seva anul·lació per pèrdua, sostracció o ús indegut; inspeccionar la correcta utilització dels títols, gestionar l'accés a títols de transport amb bonificacions socials i/o subvencions destinades a persones particulars i col·lectius concrets i posar-se en contacte amb les persones usuàries per tractar assumptes relacionats amb les seves targetes personalitzades; emetre i lliurar factures a les persones usuàries que ho sol·licitin; registrar les dades de viatges dels usuaris del Sistema Tarifari Integrat amb la finalitat de fer estadístiques.

b) Persones afectades: persones físiques o representants d'aquestes que sol·licitin una targeta de transport personalitzada amb la finalitat de carregar-hi títols de transport del sistema tarifari integrat del Camp de Tarragona, així com altres persones usuàries que sol·licitin a l'ATM l'emissió de factures corresponents a títols de transport no personalitzats.

c) Procediment de recollida: les dades s'obtenen mitjançant formularis o la transmissió electrònica de dades o documentació aportada en suport paper o via telemàtica.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o del seu representant.

e) Estructura del fitxer i tipus de dades tractades:

- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, imatge, telèfon, signatura, número d'identificació de la targeta de transport.
- *Dades de característiques personals:* sexe, data de naixement, dades familiars.
- *Dades de circumstàncies socials:* situació familiar, situació acadèmica, situació laboral, pertinença a col·lectius als quals s'aplica alguna reducció.
- *Dades ocupació laboral:* lloc de treball.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: no es preveu la cessió de dades.

h) *Transferències internacionals*: no hi ha transferència internacional de dades.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic.

2. Denominació: Contractació

a) Finalitat i usos previstos:
La finalitat del fitxer és la gestió dels contractes i dels acords i convenis de col·laboració subscrits per l'ATM del Camp de Tarragona.

Els usos del fitxer són tramitar la subscripció de contractes fins al seu total compliment: realitzar les comprovacions necessàries en fase de licitació quan escau, adjudicar el contracte, procedir a la seva formalització, fer el seguiment del contracte i les seves incidències; realitzar comandes menors i fer-ne el seguiment i portar la facturació

corresponent. Igualment, gestionar la subscripció d'acords i convenis de col·laboració per part de l'ATM i fer-ne el seguiment.

b) Persones afectades: persones físiques o representants de persones jurídiques que liciten davant l'ATM del Camp de Tarragona, i les que hi mantenen relacions contractuals i acords i convenis de col·laboració.

c) Procediment de recollida: les dades s'obtenen mitjançant comunicacions verbals, documentació aportada en suport paper o via telemàtica.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o del seu representant.

e) Estructura del fitxer i tipus de dades tractades:

- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, telèfon, signatura.
- *Dades de característiques personals:* sexe
- Dades acadèmiques i professionals: formació i titulació, experiència professional.
- *Dades d'informació comercial:* activitats i negocis.
- *Dades economicofinanceres i d'assegurances*: ingressos i rendes, dades bancàries, assegurances i avals.
- *Dades de transaccions:* béns i serveis subministrats per l'afectat.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: es preveu la cessió de dades al Registre Públic de Contractes de la Generalitat de Catalunya, d'acord amb l'article 333 del text refós de la Llei de Contractes del Sector Públic, aprovat pel Reial decret legislatiu 3/2011, de 14 de novembre. Es preveu també la comunicació de dades de caràcter personal a l'Agència Estatal d'Administració Tributària, d'acord amb la Llei 58/2003, de 17 de desembre, general tributària.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:

Consorci del Transport Públic de del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic.

3. Denominació: **Registre d'entrada i sortida**

a) Finalitat i usos previstos:
La finalitat del fitxer és registrar les entrades i sortides de documents de l'ATM.

Els usos del fitxer són la gestió i indexació dels documents com ara correspondència, sol·licituds i oficis, que es registren d'entrada i de sortida a l'ATM.

b) Persones afectades: persones físiques i representants de persones jurídiques que mantenen intercanvi documental amb l'ATM.

c) Procediment de recollida: les dades s'obtenen directament dels documents rebuts i/o emesos per l'ATM.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o del seu representant.

e) Estructura del fitxer i tipus de dades tractades:
- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, telèfon, signatura.
- *Altres dades:* dades relacionades amb el document registrat.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: no es preveu la cessió de dades.

h) *Transferències internacionals*: No hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic

4. Denominació: **Membres dels òrgans estatutaris**

a) Finalitat i usos previstos:

La finalitat del fitxer és gestionar les dades de les persones que formen part dels òrgans estatutaris de l'ATM o que hi col·laboren.

Els usos del fitxer són posar-se en contacte, mitjançant correu postal, electrònic o via telefònica, amb els membres dels òrgans estatutaris per fer-los arribar informació, convocar-los a reunions, mantenir la llista actualitzada o tractar-hi qualsevol altre tema derivat de la seva condició de ser o haver estat membre d'un dels òrgans estatutaris de l'ATM.

b) Persones afectades: persones físiques que formen part o han format part d'algun dels òrgans estatutaris de l'ATM del Camp de Tarragona, així com les persones físiques que hi col·laboren professionalment en el desenvolupament de les tasques relatives a l'ATM.

c) Procediment de recollida: les dades s'obtenen mitjançant documentació en suport paper o via telemàtica, o mitjançant conversa telefònica.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o de representants de persones jurídiques afectades; també dels estatus de l'entitat i dels acords dels òrgans estatutaris, i dels acords, decrets o resolucions de les entitats representades en aquests òrgans.

e) Estructura del fitxer i tipus de dades tractades:

- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, telèfon, signatura.
- *Dades de característiques personals:* sexe.
- *Dades d'ocupació laboral*: lloc de treball i càrrec professional a l'entitat que representa, data de designació i cessament, pertinença a òrgan estatutari, tipus d'activitat de l'òrgan estatutari.
- *Dades econòmicofinanceres*: dietes, dades bancàries.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: publicació de dades identificatives al web corporatiu amb el consentiment de la persona interessada.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic.

5. Denominació: Suggeriments, reclamacions i consultes

a) Finalitat i usos previstos:

La finalitat del fitxer és la gestió de les dades dels suggeriments, reclamacions i consultes efectuades a l'ATM.

Els usos del fitxer són tramitar el suggeriment, reclamació o consulta, derivar-lo a l'organisme competent, quan s'escaigui, i posar-se en contacte amb aquestes persones per donar-hi resposta.

b) Persones afectades: persones físiques o representants de persones jurídiques que formulin suggeriments, reclamacions i consultes a l'ATM del Camp de Tarragona.

c) Procediment de recollida: les dades s'obtenen mitjançant documentació aportada en suport paper o via telemàtica, o mitjançant conversa telefònica.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o d'altres administracions o de la Sindicatura de Greuges.

e) Estructura del fitxer i tipus de dades tractades:
- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, telèfon, signatura.
- *Dades de característiques personals:* sexe.
- *Altres dades*: fets i circumstàncies que motiven la comunicació efectuada.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: no es preveu la cessió de dades.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic

6. Denominació: Contactes

a) Finalitat i usos previstos:
La finalitat del fitxer és la gestió de les dades de les persones, l'activitat professional de les quals està directament relacionada amb l'àmbit competencial de l'ATM.

Els usos del fitxer són posar-s'hi en contacte per tractar directament assumptes professionals en què estan treballant i fer-los arribar informació sobre activitats organitzades per l'ATM.

b) Persones afectades: persones físiques o representants de persones jurídiques que es relacionen per motius professionals amb l'ATM del Camp de Tarragona.

c) Procediment de recollida: les dades s'obtenen mitjançant targetes de visita, comunicacions escrites o electròniques, converses telefòniques, entrevistes o reunions, o consultant.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o de la persona que n'ostenta la representació legal, d'entitats privades o d'administracions públiques i de fonts accessibles el públic.

e) Estructura del fitxer i tipus de dades tractades:
- *Dades identificatives:* nom i cognoms, adreça postal i electrònica, DNI/NIF/NIE/Passaport, telèfon, fax, signatura.
- *Dades de característiques personals:* sexe.
- *Dades d'ocupació laboral:* lloc de treball, càrrec.
- *Dades informació comercial:*activitats i negocis, sector d'interès.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: no es preveu la cessió de dades.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic.

7. Denominació: Recursos humans

a) Finalitat i usos previstos:

La finalitat del fitxer és la gestió dels recursos humans de l'ATM.

Els usos del fitxer són els derivats de la gestió dels recursos humans com ara la selecció i contractació del personal, la gestió de currículums, la tramitació de la nòmina, el control horari, el pagament de la Seguretat Social, la prevenció de riscos laborals, la gestió de permisos i llicències i la formació dels treballadors i les treballadores.

b) Persones afectades: Persones que presten o han prestat els seus serveis a l'ATM del Camp de Tarragona i persones interessades en treballar-hi.

c) Procediment de recollida: les dades s'obtenen mitjançant enquestes, formularis, transmissió electrònica de dades, contractes de treball i currículums, en suport paper o electrònic.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades.

e) Estructura del fitxer i tipus de dades tractades:

- *Dades identificatives:* nom i cognoms, DNI/NIF/NIE/Passaport, adreça postal i electrònica, telèfon, número Seguretat Social o mutualitat, signatura, imatge.
- *Dades de característiques personals:* sexe, data de naixement, lloc de naixement, dades familiars, nacionalitat, estat civil.
- *Dades acadèmiques i professionals:* Formació i titulacions, coneixements, experiència i perfil professional.
- *Dades d'ocupació laboral:* Cos/escala, categoria/grau, llocs de treball, història laboral, dades no econòmiques de nòmina.
- *Dades economicofinanceres i d'assegurances:* Dades bancàries, dades econòmiques de nòmina.
- *Dades relatives a la comissió d'infraccions penals o administratives:*infraccions i sancions.
- *Dades especialment protegides:*grau de disminució, aptitud del treballador/a per desenvolupar les tasques pròpies del lloc de treball, dades de salut.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: es preveu la comunicació de dades de caràcter personal a l'Agència Estatal d'Administració Tributària, d'acord amb la Llei 58/2003, de 17 de desembre, General Tributària; a la Tresoreria General de la Seguretat Social, d'acord amb el Reial decret legislatiu 1/1994, de 20 de juny, pel qual s'aprova el Text refós de la Llei general de la Seguretat Social; i a bancs i caixes, d'acord amb l'article 11.2.c) de la Llei Orgànica 15/1999, de 13 de desembre, que regula la Protecció de Dades de Caràcter Personal.
Es preveu la cessió de dades de caràcter personal al Servei d'Ocupació de Catalunya, d'acord amb l'article 16.1. del Reial Decret Legislatiu 1/1995, de 24 de març, pel qual s'aprova el Text refós de la Llei de l'Estatut dels Treballadors.

Es preveu la comunicació de dades a l'Autoritat laboral, d'acord la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de la Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona. info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell alt.

8. Denominació: Accions promocionals

a) Finalitat i usos previstos:

La finalitat del fitxer és la gestió de les dades de les persones interessades en rebre informació i/o participar en les accions promocionals impulsades per l'ATM del Camp de Tarragona.

Els usos del fitxer són posar-s'hi en contacte per fer-los arribar informació sobre accions promocionals com ara sortejos, concursos o enquestes, així com activitats educatives i culturals vinculades a la promoció del sistema tarifari integrat de l'ATM i a la sensibilització sobre l'ús de modes sostenibles de transport. Igualment, gestionar la participació de les persones que ho desitgin en les esmentades accions promocionals.

b) Persones afectades: persones físiques o representants de persones jurídiques interessades en rebre informació i/o participar en les accions promocionals impulsades per l'ATM.

c) Procediment de recollida: les dades s'obtenen mitjançant targetes de visita, comunicacions escrites o electròniques, converses telefòniques, entrevistes o reunions.

d) Procedència de les dades: dades obtingudes directament de la persona titular de les dades o de la persona que n'ostenta la representació legal, d'entitats privades o d'administracions públiques i de fonts accessibles al públic.

e) Estructura del fitxer i tipus de dades tractades:

- *Dades identificatives:* nom i cognoms, DNI/NIF/NIE/Passaport, adreça postal i electrònica i telèfon
- *Dades de característiques personals:* sexe, data de naixement.
- *Dades acadèmiques i professionals:* formació, centre d'escolarització.
- *Dades laborals:* lloc de treball.

f) Sistema de tractament: parcialment automatitzat.

g) Cessions: es preveu la publicació de dades al web, amb el consentiment de la persona interessada o de la qual n'exerceix la representació legal.

h) *Transferències internacionals*: no hi ha transferència internacional.

i) Responsable del fitxer:
Consorci del Transport Públic del Camp de Tarragona, Autoritat Territorial de Mobilitat

j) Unitat administrativa davant la qual es poden exercir els drets d'accés, rectificació, cancel·lació i oposició:
Servei tècnic d'atenció al client ATM Camp Tarragona. Carrer Anselm Clavé, 1, 43004 Tarragona info@atmcamptarragona.cat

k*) Nivell de seguretat:* nivell bàsic.

C. ANNEX C. Descripció del sistema informàtic d'accés al fitxer

Nom de l'aplicació:	Sistema de Integració Tarifaria
Descripció:	
Tipus:	Programa a mida
Programador:	
Data de realització:	
Responsable del manteniment:	
Registre d'incidències:	
Tipus de control d'accés:	
Dades de nivell mitjà:	
Nombre d'intents fallits d'accés al sistema	
Dades de nivell alt:	
Guarda història de reintents en fitxer auxiliar (Sí/No)	

Nota: Les bases de dades que emmagatzemen dades personals i dades de viatges es guarden per separat i que només es lliguen en el "protocol de bescanvi"

D. ANNEX D. Entorn de sistema operatiu i de comunicacions del fitxer

1. Sistema Operatiu

Nom:	
Versió:	
Fabricant:	
Responsable del manteniment:	
Política de paraules de pas?:	
Periodicitat de canvi:	
Actualització:	

2. Entorn de comunicacions

Tipus de xarxa local:	
Connexió amb altres xarxes locals o WAN a través d'Internet o connexions privades?.	
Tipus de connexions:	
Es comparteixen recursos i arxius?	
Sistema de xarxa:	
Límits i abast:	
Controls d'accés al fitxer des de la xarxa:	
Sistema de xifrat utilitzat en la transmissió de dades:	

3. Representació gràfica de la xarxa corporativa

E. ANNEX E. Locals i equipament

1. Locals d'ubicació dels equips que donen suport als sistemes d'informació

Local:	
Ubicació física:	
Tipus d'accés:	
Sistema de continuïtat:	
Emmagatzematge de les còpies de seguretat:	

2. Arxiu Documental

Local:	
Ubicació física:	
Criteris d'accés:	
Criteris d'arxiu	

3. Equipament

Relació dels llocs de treball	

F. ANNEX F. Personal autoritzat per accedir al fitxer

1. Responsable del tractament

Nom	Identificació fiscal
Consorci del Transport Públic del Camp de Tarragona (ATM Camp de Tarragona)	Q4300188B

2. Responsable de seguretat

Nom	
Cognoms	

3. Responsables de la gestió dels tractament que es duen a terme a cada Servei

Nom	Cognoms	Servei

4. Administradors de sistemes i de bases de dades i manteniment dels sistemes i aplicacions

Nom	Cognoms	Servei

G. ANNEX G. Procediments de control d'accés, suport, recuperació i gestió[2]

1. Procediment d'assignació i canvi de paraules de pas

Responsable de l'assignació:	
Mètode d'assignació:	
Procediment davant situacions anòmales:	
Qui és el primer en saber-ho?:	
Quan?:	
Número d'intents permesos:	
Periodicitat del canvi:	
Apareix clarament en pantalla?	

2. Procediment de còpies de seguretat i recuperació de dades

Periodicitat:	
Procediment de reconstrucció:	
Quina autorització requereix l'execució?	
ES fa constar al Registre d'incidències?:	

3. Procediment de gestió de suports

Suports identificats per etiquetes?:	
Suports que per les seves característiques físiques no permeten la identificació del	

[2]Detallar els procediments de control d'accés, suport, recuperació i gestió

tipus d'informació que contenen	
Existeix un inventari de suports?:	
Lloc d'emmagatzematge:	
Mètode utilitzat per a l'esborrat físic:	

H.ANNEX H. Funcions i obligacions del personal

1. Funcions del responsable del fitxer

El responsable del fitxer és l'encarregat jurídicament de la seguretat del fitxer i de les mesures establertes en el present document, implantarà aquestes mesures i adoptarà aquelles que siguin necessàries per a què el personal afectat per aquest document conegui les normes que afecten al desenvolupament de les seves funcions.

Designarà al responsable de seguretat que figura a l'annex F.

2. Funcions del responsable de seguretat

És l'encarregat de coordinar i controlar les mesures definides al present document.

3. Classificació del personal d'administració o personal informàtic

Es distingeixen dues situacions diferents, que condicionen el tipus de personal que té accés al fitxer en cada cas:

- Producció habitual, sense incidències tècniques. Explotació diària.
- Errors, talls, incidències tècniques de qualsevol tipus que detenen la producció.

4. Personal autoritzat en producció habitual

En el primer cas, l'accés es limita als següents perfils:

- Usuari/Administrador del sistema.
- Operador.

5. Administradors tècnics i informàtics generals que intervenen en situacions no habituals

Quan no existeix un personal tècnic determinat que es pugui relacionar de forma directa amb un fitxer o sistema informàtic i que accedeixi habitualment a l'esmentat fitxer o sistema.

Sempre serà possible conèixer el personal que va participar amb posterioritat a la intervenció, deixant constància d'aquesta, identificant al personal tècnic, anotant-ho al Registre d'incidències.

6. Funcions dels administradors o personal informàtic

El personal que administra el sistema d'accés al fitxer es pot classificar, a la vegada, en vàries categories, que no necessariament hauran d'estar presents en tots els casos, essent en algunes ocasions assumides per una mateixa persona o persones. Aquestes categories són:

- Administradors (xarxa, sistemes operatius i bases de dades). Seran els responsables dels màxims privilegis i, per tant, de màxim risc de què una actuació errònia pugui afectar al sistema. Tindran accés al programari (programes i dades) del sistema, a les eines necessàries per dur a terme les seves funcions i als fitxers o bases de dades necessaris per resoldre els problemes que sorgeixin.
- Operadors (xarxa, sistemes operatius, bases de dades i aplicació). Les seves actuacions estan limitades a l'operació dels equips i xarxes utilitzant les eines de gestió disponibles. No han de tenir, en principi, accés directe a les dades del fitxer donat que la seva actuació no precisa d'aquest accés.
- Manteniment dels sistemes i aplicacions. Personal responsable de la resolució d'incidències que puguin sorgir a l'entorn maquinari/programari dels sistemes informàtics o de la pròpia aplicació d'accés al fitxer.
- Qualsevol altre que l'organització estableixi.

7. Obligacions del responsable del fitxer

- Implantar les mesures de seguretat establertes en aquest document.
- El responsable del fitxer haurà de garantir la difusió d'aquest document entre tot el personal autoritzat a accedir a les dades del fitxer.
- Haurà de mantenir-lo actualitzat sempre que es produeixin canvis rellevants al sistema d'informació o a l'organització d'aquest.
- Haurà d'adequar en tot moment el contingut d'aquest a les disposicions vigents en matèria de seguretat de dades.

7.1. Entorn de Sistema Operatiu i de Comunicacions

a) El responsable del fitxer aprovarà o designarà a l'administrador, que es responsabilitzarà del sistema operatiu i de comunicacions i que haurà d'estar relacionat a l'annex F.

b) En el cas més simple, com és que el fitxer es trobi ubicat en un ordinador personal i accedit mitjançant una aplicació local, l'administrador del sistema operatiu podrà ser el mateix usuari que accedeix usualment al fitxer.

7.2. Sistema Informàtic o aplicacions d'accés al fitxer

a) El responsable del fitxer s'encarregarà de què els sistemes informàtics d'accés al fitxer tinguin el seu accés restringit mitjançant un codi d'usuari i una paraula de pas.

b) A la vegada, vetllarà perquè tots els usuaris autoritzats per accedir al fitxer, relacionats a l'annex F, tinguin un codi d'usuari que serà únic, i que estarà associat a la paraula de pas corresponent, que només serà coneguda pel propi usuari.

7.3. Salvaguarda i protecció de les paraules de pas personals

Només les persones relacionades a l'annex F, podran tenir accés a les dades del fitxer.

7.4. Gestió de suports

La sortida de suports informàtics que continguin dades del fitxer fora dels locals on està ubicat el fitxer haurà de ser expressament autoritzada pel responsable del fitxer.

7.5. Entrada i sortida de dades per xarxa

Totes les entrades i sortides de dades del fitxer que s'efectuïn mitjançant correu electrònic es realitzaran des d'un únic compte o adreça de correu controlada per un usuari especialment autoritzat pel responsable del fitxer. Igualment, si es realitza l'entrada o sortida de dades mitjançant sistemes de transferència de fitxers per xarxa, únicament un usuari o administrador estarà autoritzat per realitzar aquestes operacions.

7.6. Procediments de recolzament i recuperació

a) El responsable del fitxer s'encarregarà de verificar semestralment la definició i correcta aplicació dels procediments de còpies de seguretat i recuperació de les dades.

b) Serà necessària l'autorització per escrit del responsable del fitxer per a la realització dels procediments de recuperació de les dades, i haurà de deixar-se constància al Registre d'incidències de les manipulacions que s'hagin realitzat per a aquestes recuperacions,

incloent la persona que va realitzar el procés, les dades restaurades i les dades que s'hagin gravat manualment en el procés de recuperació.

7.7. Controls periòdics de verificació del compliment

a) El responsable del fitxer juntament amb el responsable de seguretat, analitzaran amb una periodicitat mínima trimestral, les incidències anotades al Registre corresponent, per tal de posar les mesures correctores que limitin aquestes incidències en el futur, independentment de les mesures particulars que s'hagin adoptat en el moment en el que es van produir.

b) Com a mínim cada dos anys, es realitzarà una Auditoria, externa o interna, que dictamini el correcte compliment i l'adequació de les mesures del present Document de Seguretat a les exigències de la LOPD i del RLOPD, identificant les deficiències i proposant les mesures correctores necessàries. Els informes d'Auditoria seran analitzats pel responsable de seguretat, qui proposarà al responsable del fitxer les mesures correctores corresponents.

c) Els resultats de tots aquests controls periòdics, així com de les Auditories seran adjuntades a aquest Document de Seguretat a l'annex K.

8. Obligacions del responsable de seguretat

El responsable de seguretat coordinarà la posada en marxa de les mesures de seguretat i col·laborarà amb el responsable del fitxer en la difusió del Document de seguretat i controlant el compliment d'aquestes.

8.1. Gestió d'incidències

a) El responsable de seguretat habilitarà un Registre d'incidències a disposició de tots els usuaris i administradors del fitxer amb la finalitat de què es registri en aquest qualsevol incidència que pugui suposar un perill per a la seguretat d'aquest.

b) Analitzarà les incidències registrades, prenent les mesures oportunes en col·laboració amb el responsable del fitxer.

8.2. Controls periòdics de verificació del compliment

a) El responsable de seguretat comprovarà, amb una periodicitat trimestral com a mínim, que la llista d'usuaris autoritzats a l'annex F es correspon amb la llista dels usuaris realment autoritzats a l'aplicació d'accés al fitxer, per al que demanarà la llista d'usuaris i els seus codis d'accés a l'administrador o administradors del fitxer. A més d'aquestes

comprovacions periòdiques, l'administrador comunicarà al responsable de seguretat, tant bon punt es produeixi, qualsevol alta o baixa d'usuaris amb accés autoritzat al fitxer.

b) Es comprovarà també, com a mínim amb periodicitat semestral, l'existència de còpies de seguretat que permetin la recuperació dels fitxers segons el que estipula l'apartat 6 d'aquest document.

c) A la vegada, i també amb periodicitat trimestral com a mínim, els administradors del fitxer comunicaran al responsable de seguretat qualsevol canvio que s'hagi realitzat a les dades tècniques dels annexos, com per exemple canvis en el programari o maquinari, bases de dades o aplicació d'accés al fitxer, procedint igualment a l'actualització d'aquests annexos.

d) El responsable de seguretat verificarà, amb una periodicitat mínima trimestral, el compliment del previst als apartats 7 i 8 d'aquest document en relació amb les entrades i sortides de dades, siguin per xarxa o en suport magnètic.

e) El responsable del fitxer, juntament amb el responsable de seguretat, analitzarà com a mínim amb periodicitat trimestral, les incidències anotades al Registre corresponent, per tal de posar les mesures correctores que limitin aquestes incidències en el futur, independentment de les mesures particulars que s'hagin adoptat en el moment en el que es van produir.

f) Com a mínim cada dos anys, es realitzarà una Auditoria, externa o interna, que dictamini el correcte compliment i l'adequació de les mesures del present Document de Seguretat a les exigències de la LOPD i del RLOPD, identificant les deficiències i proposant les mesures correctores necessàries. Els informes d'Auditoria seran analitzats pel responsable de seguretat, qui proposarà al responsable del fitxer les mesures correctores corresponents

g) Els mecanismes que permeten el registre d'accés estaran sota el control directe del responsable de seguretat sense que es permeti, en cap cas la desactivació d'aquests.

h) El responsable de seguretat s'encarregarà de revisar periòdicament la informació de control registrada i elaborarà, com a mínim mensualment, un informe de les revisions realitzades i els problemes detectats.

i) Els resultats de tots aquests controls periòdics, així com de les Auditories seran adjuntats a aquest Document de Seguretat a l'annex K.

9. Obligacions que afecten a tot el personal

9.1. Llocs de treball

a) Els llocs de treball estaran sota la responsabilitat d'algun usuari autoritzat que garantirà que la informació que mostren no pugui ser visible per persones no autoritzades.

b) Això implica que tant les pantalles com les impressores i altres tipus de dispositius connectats al lloc de treball hauran d'estar físicament ubicats a llocs que garanteixin aquesta confidencialitat.

c) Quan el responsable d'un lloc de treball l'abandoni, bé temporalment o en finalitzar el seu torn de treball, haurà de deixar-ho en un estat que impedeixi la visualització de les dades protegides. Això podrà realitzar-se a través d'un protector de pantalla, de manera que per reprendre el treball s'hagi de procedir a la desactivació de la pantalla protectora amb la introducció de la paraula de pas corresponent.

d) En el cas de les impressores haurà d'assegurar-se de què no queden documents impresos a la safata de sortida que continguin dades protegides. Si les impressores són compartides amb altres usuaris no autoritzats per accedir a les dades de fitxer, els responsables de cada lloc hauran de retirar els documents conforme vagin imprimint-se.

e) Queda expressament prohibida la connexió a xarxes o sistemes exteriors dels llocs de treball des dels quals es realitza l'accés al fitxer. La revocació d'aquesta prohibició serà autoritzada pel responsable del fitxer, quedant constància d'aquesta modificació al Registre d'incidències.

f) Els llocs de treball des dels quals es té accés al fitxer tindran una configuració fixa a les seves aplicacions i sistemes operatius que només podrà ser canviada sota l'autorització del responsable de seguretat o per administradors autoritzats a l'annex F.

9.2. Salvaguarda i protecció de les paraules de pas personals

Cada usuari serà responsable de la confidencialitat de la seva paraula de pas i, en cas de què aquesta sigui coneguda fortuïtament o fraudulentament per persones no autoritzades, haurà de registrar-ho com a incidència i procedir al seu canvi.

9.3. Gestió d'incidències

a) Qualsevol usuari que tingui coneixement d'una incidència és responsable de la comunicació d'aquesta a l'administrador del sistema, o en el seu caso del registre d'aquestes al sistema de Registre d'incidències del fitxer.

b) El coneixement i la no notificació d'una incidència per part d'un usuari serà considerat com una falta contra la seguretat del fitxer per part d'aquell usuari.

9.4. Gestió de suports

a) Els suports que continguin dades del fitxer, bé com a conseqüència d'operacions intermèdies pròpies de l'aplicació que les tracta o com a conseqüència de processos periòdics de recolzament o qualsevol altra operació esporàdica, hauran d'estar clarament identificats amb una etiqueta externa que indiqui de quin fitxer es tracta, quin tipus de dades conté, procés que les ha originat i data de creació.

b) Aquells mitjans que siguin reutilitzables, i que hagin contingut còpies de dades del fitxer, hauran de ser esborrats físicament abans de la seva reutilització, de forma que les dades que contenien no puguin ser recuperades.

c) Els suports que continguin dades del fitxer hauran de ser emmagatzemats en llocs als que no tinguin accés persones no autoritzades per a l'ús del fitxer, les quals no estiguin relacionades a l'annex F.

d) Quan la sortida de dades del fitxer es realitzi per mitjà de correu electrònic, els enviaments es realitzaran, sempre i únicament, des d'una adreça de correu controlada per l'administrador de seguretat, deixant constància d'aquests enviaments al directori històric de dita adreça de correu o en un altre sistema de registre de sortides que permeti conèixer en qualsevol moment els enviaments realitzats, a qui anaven dirigits i la informació enviada.

e) Quan les dades del fitxer hagin d'enviar-se fora del recinte físicament protegit on es troba ubicat el fitxer, bé sigui mitjançant un suport físic de gravació de dades o mitjançant correu electrònic, hauran de ser encriptades, de forma que només puguin ser llegides i interpretades pel seu destinatari.

f) S'hauran de registrar mitjançant correu electrònic o transferència de dades per xarxa, de forma que es pugui sempre identificar el seu origen, tipus de dades, format, data i hora de l'enviament i destinatari d'aquestes.

10. Obligacions dels administradors i personal informàtic

10.1. Entorno de sistema operatiu i de comunicacions

a) Cap eina o programa d'utilitat que permeti l'accés al fitxer haurà de ser accessible a un usuari o administrador no autoritzat a l'annex F.

b) A la norma anterior s'inclou qualsevol mitjà d'accés en brut, és a dir no elaborat o editat, a les dades del fitxer, como les anomenades queries, editors universals, analitzadors de fitxers, etc., que hauran d'estar sota el control dels administradors autoritzats i relacionats a l'annex F.

a) L'administrador haurà de responsabilitzar-se de guardar en un lloc protegit les còpies de seguretat i recolzament del fitxer, de forma que cap persona no autoritzada tingui accés a aquestes.

b) Si l'aplicació o sistema d'accés al fitxer utilitzés usualment fitxers temporals, fitxers de logging o qualsevol altre mitjà en el que puguin ser gravades còpies de les dades protegides, l'administrador haurà d'assegurar-se de què aquestes dades no són accessibles posteriorment per personal no autoritzat.

c) Si l'ordinador en el que està ubicat el fitxer està integrat en una xarxa de comunicacions, de forma que des d'altres ordinadors connectats a aquesta sigui possible l'accés al fitxer, l'administrador responsable del sistema haurà d'assegurar-se de què aquest accés no es permet a persones no autoritzades.

10.2.Sistema Informàtic o aplicacions d'accés al fitxer

a) Si l'aplicació informàtica que permet l'accés al fitxer no compta amb un control d'accés, haurà de ser el sistema operatiu, on s'executa aquella aplicació, el que impedeixi l'accés no autoritzat mitjançant el control dels citats codis d'usuari i paraules de pas.

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

c) Si durant les proves anteriors a la implantació o modificació de l'aplicació d'accés al fitxer s'utilitzessin dades reals, s'haurà d'aplicar a aquests fitxer de prova el mateix tractament de seguretat que s'aplica al fitxer, i s'hauran de relacionar els fitxers de prova a l'annex B.

10.3.Salvaguarda i protecció de les paraules de pas personals

a) Les paraules de pas s'assignaran i canviaran mitjançant el mecanisme i periodicitat que es determina a l'annex G. Aquest mecanisme d'assignació i distribució de les paraules de pas haurà de garantir la confidencialitat d'aquestes i serà responsabilitat de l'administrador del sistema.

b) L'arxiu on s'emmagatzemen les paraules de pas haurà d'estar protegit i sota la responsabilitat de l'administrador del sistema.

10.4. Procediments de recolzament i recuperació

a) Existirà una persona, sigui l'administrador o bé un altre usuari expressament designat, que serà responsable d'obtenir periòdicament una còpia de seguretat del fitxer, a efectes de recolzament i possible recuperació en caso de fallada.

b) Aquestes còpies hauran de realitzar-se amb una periodicitat mínima setmanal, excepte en el cas que no s'hagi produït cap actualització de les dades.

c) En cas de fallada del sistema amb pèrdua total o parcial de les dades del fitxer existirà un procediment, informàtic o manual, que partint de la darrera còpia de seguretat i del registre de les operacions realitzades des del moment de la còpia, reconstrueixi les dades del fitxer a l'estat en què es trobaven en el moment de la caiguda. Aquest procediment està descrit a l'annex G.

d) Serà necessària l'autorització per escrit del responsable del fitxer per a l'execució dels procediments de recuperació de les dades i haurà de deixar-se constància al Registre d'incidències de les manipulacions que hagin estat necessàries per realitzar aquestes recuperacions, incloent la persona que va realitzar el procés, les dades restaurades i les dades que en el procés de recuperació hagin estat gravades manualment.

10.5. Controls periòdics de verificació del compliment

A. El responsable de seguretat comprovarà, amb una periodicitat mínima trimestral, que la llista d'usuaris autoritzats a l'annex F es correspongui amb la llista dels usuaris realment autoritzats a l'aplicació d'accés al fitxer, per al que demanarà la llista d'usuaris i dels seus codis d'accés a l'administrador o administradors del fitxer. A més d'aquestes comprovacions periòdiques, l'administrador comunicarà al responsable de seguretat, en el moment en que es produeixi, qualsevol alta o baixa d'usuaris amb accés autoritzat al fitxer.

B. Es comprovarà també, com a mínim de manera trimestral, l'existència de còpies de seguretat que permetin la recuperació del fitxer segon el que s'estipula a l'apartat 8 d'aquest document.

C. A la vegada, i també amb una periodicitat mínima trimestral, els administradors del fitxer comunicaran al responsable de seguretat qualsevol canvi que s'hagi realitzat a les dades tècniques dels annexos, como per exemple canvis en el programari o maquinari, base de dades o aplicació d'accés al fitxer, procedint igualment a l'actualització d'aquests annexos.

D. El responsable de seguretat verificarà, com a mínim amb periodicitat trimestral, el compliment del previst als apartats 7 i 8 d'aquest document en relació amb les entrades i sortides de dades, siguin per xarxa o en suport magnètic.

E. Es realitzarà una Auditoria externa o interna, com a mínim de manera biennal, que dictamini el correcte compliment i l'adequació de les mesures del present Document de Seguretat a les exigències de la LOPD i del RLOPD, identificant les deficiències i proposant les mesures correctores necessàries. Els informes d'Auditoria seran analitzats pel responsable de seguretat, que proposarà al responsable del fitxer les mesures correctores corresponents.

F. Els mecanismes que permeten el registre d'accés estaran sota el control directe del responsable de seguretat sense que es permeti, en cap cas la desactivació d'aquests.

G. El responsable de seguretat s'encarregarà de revisar periòdicament la informació de control registrada i elaborarà un informe de les revisions realitzades i els problemes detectats com a mínim mensualment.

H. Els resultats de tots aquests controls periòdics, així com de les Auditories seran adjuntats a aquest Document de Seguretat a l'annex K.

I. ANNEX I. Procediment de notificació i gestió d'incidències

J. ANNEX J. Relació de contractes amb tercers amb accés als fitxers[3]

1. Relació dels tercers que tracten les dades a les instal·lacions de l'ATM

NOM DE L'EMPRESA (Encarregat del tractament)	
Descripció del tractament encomanat	
Ubicació on es tractaran les dades	
FITXERS	
Nom dels fitxers als que accedeix i nivell de seguretat	
CONTRACTE	
Núm. de referència del contracte	
Data d'entrada en vigor del contracte	
Data de finalització del contracte	

[3]Formaran part d'aquest document, com a annexos al mateix, els documents que permetin acreditar la celebració i contingut dels contractes d'encarregat de tractament amb els tercers les dades dels quals consten en aquest informe.

2. Relació dels tercers que accedeixen als sistemes d'informació de l'ATM amb accés remot

NOM DE L'EMPRESA (Encarregat del tractament)	
Descripció del tractament encomanat	
Ubicació on es tractaran les dades	
FITXERS	
Nom dels fitxers als que accedeix i nivell de seguretat	
CONTRACTE	
Núm. de referència del contracte	
Data d'entrada en vigor del contracte	
Data de finalització del contracte	

3. Relació dels tercers que tracten les dades a les seves instal·lacions

NOM DE L'EMPRESA (Encarregat del tractament)	
Descripció del tractament encomanat	
Ubicació on es tractaran les dades	
FITXERS	
Nom dels fitxers als que accedeix i nivell de seguretat	
CONTRACTE	
Núm. de referència del contracte	
Data d'entrada en vigor del contracte	
Data de finalització del contracte	

K. ANNEX K. Controls periòdics i auditories

1. Relació d'actualitzacions

Data	Aspectes modificats

2. Auditories realitzades

Data	Empresa	Control
03/11/2016	APDCAT	5è pla d'Auditoria de Protecció de Dades de caràcter personal