Càritas
Mataró

Manual de Seguretat de l'agent de CÀRITAS DE MATARÓ

CONTINGUT

1. INTRODUCCIÓ

La dignitat és el valor absolut que té cada ésser humà per ser criatura de Déu. És un atribut de la naturalesa humana racional i lliure. CÀRITAS MATARÓ, entitat de l'Església Catòlica, reconeix "el dret de cada persona a protegir la seva pròpia intimitat" (cànon 220 del Codi de Dret Canònic, 1983). És un dret natural, que també forma part dels Drets Humans i que, per tant, ha de ser respectat. El reconeixement de la dignitat de la persona i la seva intimitat inclou també una protecció adequada de les seves dades personals. Constitueix a més un dret fonamental reconegut per la Constitució Espanyola (art. 18.4) pel qual es garanteix a la persona el control sobre les seves dades, sobre el seu ús i destí.

Dins dels valors de CÀRITAS MATARÓ es recull, d'una banda, la centralitat de la persona, això és, la persona com a centre de l'acció de Càritas i la defensa de la seva dignitat, i d'altra banda, la transparència, com a obertura de la informació a tots els interessats en la labor de Càritas. La informació és un dels principals actius de CÀRITAS MATARÓ i, com a tal actiu, està exposat a riscos i amenaces que poden provenir des de dins o fora de l'organització, i poden ser intencionals o accidentals.

Com a Responsable de Tractament, CÀRITAS MATARÓ (NIF R-0800544-I) és plenament conscient de la importància de protegir les dades personals que es tracten en el seu sistema d'informació. De fet, la protecció d'aquestes dades, que es tracten sota la seva responsabilitat, és un objectiu prioritari en l'àmbit de gestió d'aquesta entitat.

Amb la finalitat que els agents de CÀRITAS MATARÓ -ja sigui amb vinculació laboral o bé com a voluntaris, becaris i persones en pràctiques- disposin d'una eina que faciliti el coneixement i compliment de les normes bàsiques en matèria de seguretat de la informació i, en particular, de les dades personals, es posa a la disposició de tots els agents el present Manual de Seguretat de l'agent de CÀRITAS MATARÓ (d'ara endavant, el "Manual").

Aquest Manual respon al que es disposa en la legislació aplicable a CÀRITAS MATARÓ en matèria de protecció de dades personals. És a dir:

- Reglament (UE) 2016/679, General de Protecció de Dades (*RGPD),
- Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPD-GDD), i
- Decret General de la Conferència Episcopal Espanyola sobre la Protecció de Dades de l'Església Catòlica a Espanya de 22 de maig de 2018 (DGPD-CEE).

2. OBJECTE I ABAST

Objecte: El present Manual és un instrument informatiu de CÀRITAS MATARÓ mitjançant el qual es pretén donar a conèixer als seus agents, les normes bàsiques en matèria de seguretat de la informació i protecció de dades de caràcter personal, així com conscienciar sobre la importància de protegir els recursos.

Per a dur a terme aquest propòsit el punt de partida passa per la definició i comprensió del concepte de "dades personals" i, en segon lloc, conèixer els destinataris i l'àmbit al qual es refereix aquest Manual.

Dades personals: aquelles dades en qualsevol format formades per qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que es refereixi a persones físiques identificades o que puguin ser identificables.

Abast: L'àmbit d'aplicació del present manual es desplega en una doble vessant, objectiva i subjectiva:

Àmbit objectiu

Conjunt d'elements físics i lògics integrats en el sistema d'informació de CÀRITAS MATARÓ. Això inclou:

- Maquinari (PC, portàtils, tauletes, telèfons mòbils, impressores, etc.).
- Programari i bases de dades (correu electrònic, Internet, Intranet, etc.).
- Dispositius d'emmagatzematge principal i auxiliar (discos durs, USB, cd, etc.).
- CPD/ locals/ oficines.
- Arxius i registres en suport paper i en formats analògics.

Àmbit subjectiu

Conjunt d'usuaris del sistema d'informació obligats al compliment del present Manual. Aquest conjunt d'usuaris està constituït fonamentalment pels agents de CÀRITAS MATARÓ; és a dir, les persones que presten serveis per a CÀRITAS MATARÓ ja sigui sobre la base de l'existència d'un contracte laboral (treballadors), de l'existència d'un acord d'incorporació de voluntariat (voluntaris) o bé d'un acord amb la Universitat i/o Centres de Formació Professional (becaris i alumnes en pràctiques).

Les normes contingudes en el present Manual també podran ser aplicables, subsidiàriament, a les relacions amb proveïdors de serveis auxiliars externs amb accés a dades personals (encarregats de tractament), sense perjudici del contingut dels contractes subscrits entre aquests i CÀRITAS MATARÓ.

Un **agent de Càritas** és, doncs, tota persona que col·labora amb Càritas, sigui voluntari, contractat, becari o alumne en pràctiques.

Càritas, a través dels seus agents, ha de vetllar per la protecció de dades personals, per la transparència i seguretat cap a les persones que atén i acompanya i cap a les persones que col·laboren amb nosaltres, per la qual cosa, en cap moment, poden descurar els agents les seves obligacions cap a les persones i les lleis en vigor relatives a drets d'intimitat i privacitat.

En última instància, és el Consell Directiu de CÀRITAS MATARÓ, la que estableix els criteris d'accés a quins recursos de Càritas i en quines condicions.

3. PRINCIPIS RECTORS RELATIUS AL TRACTAMENT DE LES DADES PERSONALS

- Les dades personals han de tractar-se de manera lícita i transparent, garantint la lleialtat i el respecte cap a les persones les dades personals de les quals s'estan tractant.
- L'obtenció i, en general, el tractament de les dades personals ha d'obeir a finalitats específiques; és a dir, no poden recopilar-se dades personals per a fins indeterminats, ni es poden utilitzar les dades personals per a altres fins que no siguin compatibles amb la finalitat original de la recopilació.
- Només han de recollir-se i tractar-se les dades personals que siguin necessaris per al compliment de les finalitats específiques per a les quals van ser obtingudes.
- Les dades personals objecte de tractament hauran de ser exactes i mantenir-se actualitzades.
- Les dades personals no es conservaran més temps del necessari per als fins per als quals van ser recopilades.
- Les dades personals han de ser protegides a través de mesures tècniques i organitzatives dirigides a evitar el tractament no autoritzat o il·lícit d'aquests, així com la seva pèrdua, destrucció o dany, ja sigui a conseqüència d'accidents o d'actuacions intencionades o negligents.

4. NORMES BÀSIQUES D'ÚS DEL SISTEMA D'INFORMACIÓ

Conforme a la Política de Seguretat de la Informació i de Privacitat, es desenvolupa a continuació un catàleg de normes d'ús diligent i bones pràctiques dels sistemes d'informació amb la finalitat de protegir dades personals i prevenir riscos i amenaces que poden ser intencionals o accidentals procedents des de fora o fins i tot des de dins de l'organització.

Aquestes normes d'ús s'estructuren entorn de quatre apartats rellevants:

- Tractament de dades personals.
- Dispositius.
- Aplicacions.
- Informació en paper de dades personals.

Així mateix, i amb caràcter complementari, s'adjunten com a annex a aquest Manual uns criteris generals per a l'ús de dispositius i aplicacions d'acord amb el Codi de Conducta de CÀRITAS MATARÓ i l'ús inadequat dels quals pot repercutir en la protecció de dades personals, en la generació d'incidències en els sistemes d'informació i, fins i tot, perjudicar la reputació de Càritas. Aquests criteris s'organitzen en quatre apartats importants:

- Altres dispositius.
- Internet.
- Correu electrònic.
- Informació en paper.

TRACTAMENT DE DADES PERSONALS

Deure de secret i confidencialitat

Els agents estan obligats a complir el deure de confidencialitat i, en el seu cas, el deure de secret professional, en relació amb les dades personals als quals poguessin tenir accés en l'àmbit de CARITAS INTERPARROQUIAL MATARÓ, comprometent-se a no divulgar-les, publicar-les, revelar-les ni de forma directa o indirecta posar-les a la disposició de persones que no estiguin autoritzades a accedir a aquestes.

Creació i autorització de nous tractaments de dades

Únicament les persones designades com a Administradors de RAT (Registres d'Activitat de Tractament) estan autoritzades per a crear o autoritzar nous tractaments de dades personals. En particular, no es podrà recaptar en cap concepte dades personals fora dels procediments previstos, crear bases de dades personals no expressament autoritzades o procedir a fer altres tasques similars sense la deguda autorització.

Aquesta obligació subsistirà fins i tot després de la finalització de la relació de cada agent amb CÀRITAS INTERPARROQUIAL MATARÓ, respecte de les dades als quals hagi tingut accés durant l'acompliment de les seves funcions.

Dades personals en registres o fitxers temporals

Els registres o fitxers temporals són fitxers de treball creats per agents o processos que són necessaris per a un tractament de dades personals ocasional o com a pas intermedi durant la

realització d'un tractament. Aquests fitxers temporals normalment s'efectuen en un documents de text o un full de càlcul. Exemples:

- Llista de donants que es pugui crear en un full de càlcul per a enviar-los una actualització d'informació fiscal, i que després no es torna a utilitzar. O l'ús d'aquest mateix full de càlcul per a exportar les dades que conté a una base de dades permanent a SICCE.
- Creació d'un fitxer temporal en un document de text per a organitzar les vacances dels agents a partir del fitxer de Desenvolupament de persones.

Una vegada s'ha utilitzat, ha de ser esborrat o destruït, i encara que siguin temporals, hauran de complir amb les mesures de seguretat que els correspongui d'acord amb les dades que continguin.

Criteris:

a) **Ubicació:** Cal desar els fitxers temporals a la carpeta de la unitat "CIM" assignada a tal efecte. Carpeta només accessible amb els permisos assignats a cada usuari segons tasques.

b) **Creació:** L'agent no crearà fitxers temporals o còpies de documents (creats per a un tractament ocasional o com a pas intermedi durant la realització d'un altre tractament) tret que resulti estrictament necessari per al desenvolupament de les seves funcions.

c) **Mesures de seguretat:** l'agent haurà d'aplicar sobre els fitxers temporals o còpies de documents creats les mateixes mesures de seguretat que corresponguin als fitxers o documents originals. Es destaca a tall d'exemple que els fitxers d'usuaris o beneficiaris de Càritas com SICCE-Mòdul d'Intervenció Social els són aplicables les mesures de seguretat que corresponen a dades personals de categoria especial (sensibles o confidencials).

d) **Actualització i esborrament:** l'agent haurà de mantenir les dades registrades en els fitxers temporals o còpies de documents permanentment actualitzades. Una vegada que hagin deixat de ser necessàries per a la fi que van motivar la seva creació, l'agent haurà d'esborrar o destruir els fitxers temporals o còpies de documents.

e) **Destrucció:** l'agent haurà d'eliminar a través dels mecanismes habilitats per a la seva destrucció, qualsevol document en suport paper que contingui dades personals una vegada que deixi d'estar en ús.

Ús responsable de dispositius digitals

Els agents de CÀRITAS MATARÓ únicament tractaran dades personals que estiguin sota la responsabilitat d'aquesta entitat mitjançant dispositius digitals prèviament subministrats o autoritzats per aquesta. En tot cas, els dispositius digitals utilitzats en el tractament de dades personals sota responsabilitat de CÀRITAS MATARÓ hauran d'estar protegits mitjançant contrasenyes personals que seran creades i gestionades d'acord amb la política de gestió de contrasenyes descrita en el present document. I en particular, els ordinadors portàtils subministrats per l'entitat estaran prèviament encriptats com s'indica en l'apartat d'encriptació.

Gestió de contrasenyes

Tots els agents de CÀRITAS MATARÓ que siguin usuaris autoritzats del sistema informàtic integrat en el sistema d'informació d'aquesta entitat han de disposar de contrasenyes personals

d'accés als diferents recursos. Aquestes contrasenyes han de ser gestionades pels agents com s'indica a continuació:

a. Sempre que sigui possible, per a l'establiment de contrasenyes personals d'accés a dades personals sota responsabilitat de CÀRITAS INTERPARROQUIAL MATARÓ es compliran els següents requisits:
   - ✓ La longitud mínima de la contrasenya ha de ser de vuit caràcters.
   - ✓ La contrasenya ha de tenir una lletra majúscula, una lletra minúscula, un dígit i un símbol no alfanumèric (& % $ @ …)
   - ✓ Les contrasenyes no han d'incloure noms propis.
   - ✓ Les contrasenyes no poden consistir solament en dates.
   - ✓ No podrà ser igual a cap de les tres últimes contrasenyes anteriorment utilitzades.

   Com a suggeriment per a l'establiment de contrasenyes segures i fàcils de recordar: s'aconsella utilitzar el mètode de les "frases contrasenya". Es tracta d'una expressió familiar en la qual es canvien alguns caràcters per altres per tal de fer-la irreconeixible. Per exemple: "Qui no té cap, ha de tenir cames" es pot convertir en "Qu1.n0.t3.c4p@.h4.d3.t3n1r.c4m3s" només reemplaçant la lletra "a" per un 4 (A→4), la "e" per un 3 (E→3), la "i" per un 1 (I→1), la "o" per un 0 (O→0), la "," per un "@" i els " " per un punt, deixant-la irreconeixible i prou llarga per ser una contrasenya forta.

b. Els agents només accediran als recursos necessaris per al desenvolupament de les funcions que tingui assignades. En cas de no disposar de contrasenyes operatives d'accés, els agents hauran de sol·licitar-les al seu superior i mai utilitzar vies alternatives d'accés.
c. Quan es registra un nou usuari en el sistema, se li assigna una contrasenya per defecte que ha de ser modificada per l'agent en el seu primer accés al sistema.
d. Les contrasenyes són personals i intransferibles. Mai ha de facilitar-se la contrasenya absolutament a ningú, sota cap concepte.
e. Les contrasenyes personals d'accés tenen establert un període de vigència, transcorregut el qual es produirà la caducitat de les mateixes, pel que s'haurà de procedir a crear una nova contrasenya. No obstant això, si un agent considera que la seguretat de la seva contrasenya pot estar compromesa, haurà d'establir i/o sol·licitar una nova contrasenya malgrat no haver transcorregut el termini de vigència.
f. Haurà d'evitar-se la configuració dels navegadors d'acord amb l'opció de "recordar contrasenyes".

Com guardar informació en el PC

A fi d'assegurar la disponibilitat de la informació relativa a dades personals i de disposar de còpia de seguretat, la informació amb la qual es treballa haurà de guardar-se al disc de dades CIM del servidor de CÀRITAS MATARÓ.

Fora de la ubicació referida: unitat de disc CIM, existeix un alt risc de pèrdua d'informació ja que no existeix còpia de seguretat.

Encriptació d'equips

L'agent haurà de vetllar per la seguretat i confidencialitat de la informació continguda en els equips, sobretot quan es trobi fora de les dependències de CÀRITAS MATARÓ. Els discos durs

dels ordinadors portàtils podran ser xifrats, sempre d'acord amb el pla de xifratge desenvolupat per CÀRITAS MATARÓ i en la mesura que els equips ho permetin. L'agent haurà de gestionar aquesta informació utilitzant els mecanismes que CÀRITAS MATARÓ determini, sobre els que l'informarà i formarà adequadament.

Instal·lació d'aplicacions

L'agent no haurà d'instal·lar en cap concepte, per si mateix i sense la deguda autorització, aplicacions en els equips proveïts per CÀRITAS MATARÓ, especialment amb la finalitat de salvaguardar i protegir la integritat de les dades personals. Aquesta prohibició és extensible a les aplicacions portables (que no requereixen instal·lació).

En cas de precisar una aplicació no disponible, haurà de sol·licitar la instal·lació de la mateixa a l'Equip de Gestió de la Informació, des d'on s'adoptarà la decisió oportuna.

L'agent no haurà de traspassar de cap manera els permisos del seu compte, especialment per a instal·lar aplicacions no relacionades amb el treball.

No es podrà realitzar qualsevol alteració de l'arrencada o de la seva seqüència habitual per a accedir a un compte sense disposar de contrasenya.

Dispositius portàtils o extraïbles (USB, targetes de memòria)

Per a protegir la informació propietat de CÀRITAS MATARÓ és necessari controlar els dispositius d'emmagatzematge extraïbles (claus USB, discos durs portàtils, targetes de memòria, etc.).

L'ús d'emmagatzematge USB (o pendrive) és un dels principals punts d'entrada de programari mal intencionat.

Els agents han de ser conscients que només introduint un USB en el seu equip es pot estar recopilant informació sense adonar-se d'això. En cas de necessitar enviar o rebre fitxers, utilitzar mitjans més segurs com el correu electrònic o desar-la a la carpeta adient del disc CIM per tal que els usuaris que hagin d'accedir ho puguin fer.

S'evitarà l'ús de dispositius extraïbles. L'Equip de Gestió de la Informació no disposa de dispositius extraïbles. Si fos estrictament necessari l'ús d'alguna mena d'emmagatzematge USB, serà l'agent qui ha de garantir la seguretat d'aquest.

En cap cas està permesa la sortida/ entrada de suports amb dades de caràcter personal a l'exterior sense la prèvia autorització i registre d'aquests. En cas de pèrdua o robatori d'algun d'aquests dispositius l'agent comunicarà la incidència al Responsable de Seguretat.

Ús del correu electrònic amb dades personals

Amb caràcter general, l'agent evitarà l'enviament de dades personals de categoria especial (especialment sensibles) mitjançant correu electrònic. En cas de ser necessari tal enviament, les dades hauran de ser xifrats[1].

[1] *Xifratge: transformació de la informació mitjançant un algorisme que utilitza una clau de xifratge. Sense aquesta clau la informació no pot ser desxifrada i, per tant, accessible.*

Informació impresa amb Dades Personals extretes de SICCE

Escriptoris nets

Tots els usuaris han de seguir les següents normes sobre la informació impresa en paper que conté dades de caràcter personal:

- Ha de ser retornada sempre al seu lloc d'emmagatzematge quan s'acabi d'usar, no deixant cap documentació confidencial damunt de l'escriptori sense atenció. En cas que s'hagi enviat fax o es realitzin fotocòpies/escanejat de documents, s'ha de retirar immediatament del dispositiu corresponent, retornant-lo al seu lloc d'emmagatzematge.
- En cap cas han de quedar sobre els escriptoris documents que continguin informació amb dades personals, especialment aquells que incloguin dades de categoria especial o confidencial (salut, religió, discapacitat, orientació sexual, condemnes i infraccions penals, afiliació sindical, etc.).

En cas d'imprimir informació amb dades personals de categoria especial o confidencial, assegurar-se que s'envia a la impressora desitjada i es recull de seguida.

Una vegada acabades les tasques per a les quals van ser impresos, els documents que continguin dades de caràcter personal hauran de desar-los a les capses d'eliminació de documents de la seu.

Per als enviaments per correu postal, no s'utilitzarà el correu ordinari per a l'enviament d'informació amb dades de categoria especial, sinó que s'utilitzaran alternatives segures: correu certificat o missatgeria.

Ús de la impressora, fotocopiadora i escàner

En tot cas, l'agent s'assegurarà que no quedin documents impresos en la safata de sortida o retinguts en la cua d'impressió que continguin dades personals, així com de retirar els documents conforme vagin sent impresos. Aquest mateix compromís s'exercirà respecte de faxos, escàner o altres dispositius d'anàloga funcionalitat.

Respecte a la informació escanejada, CÀRITAS INTERPARROQUIAL MATARÓ vetllarà el seu funcionament respecte a l'ús inadequat d'informació amb dades personals.

Una vegada acabades les tasques per a les quals van ser impresos, els documents que continguin dades de caràcter personal hauran de desar-los a les capses d'eliminació de documents de la seu.

Emmagatzematge de documents impresos amb dades personals

L'arxiu dels registres o documents amb dades personals haurà de realitzar-se per l'agent de tal manera que es garanteixi la correcta conservació dels documents, la localització i consulta de la informació i possibilitar l'exercici dels drets dels interessats.

Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin el seu accés. L'Administrador dels fitxers o registres de l'activitat de tractament de dades adoptarà mesures que impedeixin l'accés de persones no autoritzades.

Els armaris, arxivadors o altres elements en els quals s'emmagatzemin els documents impresos amb dades de caràcter personal de categoria especial (confidencials o sensibles) hauran de trobar-se en espais en les quals l'accés estigui protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent. Aquests espais hauran de romandre tancats quan no calgui l'accés als documents inclosos en el document amb dades personals.

5. GESTIÓ I COMUNICACIÓ D'INCIDÈNCIES

Incidències

Una incidència és qualsevol anomalia que afecti o pogués afectar la seguretat de les dades. Amb caràcter merament enunciatiu, i no taxatiu, es consideren incidències les següents eventualitats que poden donar lloc a violacions de seguretat de la informació:

- Incidències que afecten la identificació i autenticació:
  - Pèrdua de confidencialitat de les contrasenyes.
  - Assignació o modificació de drets sobre eines de gestió d'accés i utilitats amb accessos privilegiats.
  - Desactivació de les eines de seguretat (antivirus, navegador).
  - Les assignacions de perfils i canvis de contrasenyes per pèrdua o oblit.
- Incidències que afecten els drets d'accés a les dades:
  - Comunicació dels usuaris de sospites que algú ha suplantat la seva personalitat.
  - Detecció de punts d'accés desatesos (wifi oberta sense usuaris ni contrasenyes) i sense protecció de pantalla activada (bloqueig de sessions).
  - Detecció de contrasenyes escrites en els llocs de treball.
  - Revisió d'informes de seguretat.
  - La caiguda del sistema de seguretat informàtica, per qualsevol causa, que possibiliti l'accés a les dades personals a persones no autoritzades.
- Incidències que afecten la gestió de suports:
  - La destrucció, total o parcial, del dispositiu o suport físic (ordinador, mòbil, tauleta, paper…) de les dades personals.
  - Comunicació de pèrdua o extraviament d'ordinadors personals.
  - Comunicació de pèrdua o extraviament de dispositius o altres suports tant personals com corporatius sempre que continguin dades personals (Discos durs, USB, CD'S, cintes, etc.).
  - Comunicació de localització de dispositius en llocs inadequats.
  - Errors de contingut en dispositius rebuts.
  - Intent de sortida d'un dispositiu no autoritzat.
- Incidències que afecten els procediments de còpies de seguretat i recuperació:
  - Errors en els processos de realització de còpies de seguretat.
  - Errors en les proves dels processos de realització de còpies de seguretat i recuperació.
  - Procediments de recuperació de dades realitzades (per exemple , dades cancel·lades o esborrades anteriorment que són recuperats).
  - Pèrdua de dades motivades per causes inesperades (infeccions per virus, accidents...).
- Incidències que afecten l'exercici dels drets dels afectats:
  - Incompliment de terminis per a atendre les sol·licituds d'afectats exercitant el dret d'accés, rectificació, cancel·lació o oposició sobre les seves dades personals.
- Incidències generals sobre tractaments:
  - Creació de bases de dades de caràcter personal sense haver cursat sol·licitud al Responsable de Seguretat.
  - Ús il·lícit de dades personals.
  - Recaptar dades sense l'autorització de l'afectat quan sigui preceptiva i sense informar-lo dels seus drets.

- Ús de les dades per a una finalitat diferent de la que figura registrada en el Registre d'Activitats de Tractaments.
- Ús il·lícit de les dades de caràcter personal.

- Incidències en documents impresos amb dades personals (en paper o no automatitzats):
  - Pèrdua de claus d'accés als arxius, armaris, o dependències on es troben els registres d'activitats de tractament (fitxers) amb dades de caràcter personal.
  - Accés no autoritzat d'agents a aquests arxius, armaris o dependències.
  - Pèrdues de suports o documents en paper amb dades de caràcter personal.
  - Deterioració dels suports o documents, armaris o arxius, on es troben dades de caràcter personal.

Comunicació de les incidències

Qualsevol petició o consulta, relacionada amb la seguretat de les dades ha de ser cursada preferentment a través de correu electrònic a cbustos.cimataro@caritas.es on registrarà la incidència, amb la següent informació:

a. Data i hora en què es va produir la incidència
b. Tipologia d'incidència
c. Persona que realitza la comunicació
d. Persona(es) a qui es comunica
e. Efectes derivats de la incidència
f. Mesures correctores aplicades
g. Procediment de recuperació de les dades realitzat
h. Dades restaurades

És responsabilitat de cada usuari reportar immediatament al Gestor de Seguretat (cbustos.cimataro@caritas.es) qualsevol violació de seguretat que detecti almenys amb indicació de:

- Data i hora de la detecció de la incidència.
- Persona que notifica la incidència.
- Descripció detallada de la incidència.
- Dades recuperades (Si afecta Dades Personals, indicar si hi ha dades recuperades manualment).
- Observacions.

El coneixement i no notificació en els termes especificats anteriorment per part d'un agent es considerarà una falta contra la seguretat de la informació propietat i/o responsabilitat de CÀRITAS MATARÓ.

6. AVISOS LEGALS PER ALS AGENTS DE CÀRITAS

Drets digitals

D'acord amb el que es disposa en la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades i Garantia dels Drets Digitals (LOPD-GDD), CÀRITAS MATARÓ garantirà:

- El dret a la desconnexió digital dels agents treballadors de manera que, excepte en casos de força major o d'urgent necessitat extraordinària, una vegada finalitzada la jornada laboral, així com durant els permisos i períodes de vacances, aquests puguin gaudir del seu temps de descans, amb respecte a la seva intimitat personal i familiar i sense ingerències de l'empresa derivades de l'ús indegut dels mitjans de comunicació electrònica.
- El dret a la intimitat en relació amb l'ús dels dispositius digitals en l'àmbit laboral: El present Manual inclou les normes internes d'utilització dels serveis i dispositius digitals en l'àmbit laboral, com ara ordenadors personals, tauletes, telèfons intel·ligents, accés a Internet, càmeres de videovigilància, servei de correu electrònic i missatgeria instantània, dispositius d'emmagatzematge portàtil, etc. Aquestes normes s'han establert d'acord amb la facultat de vigilància i control empresarial reconeguda en l'article 20 de l'Estatut dels Treballadors, així com en el marc del reconeixement del dret a la intimitat en relació amb l'ús dels dispositius digitals en l'àmbit laboral, d'acord amb la LOPD-GDD.

Avís informatiu sobre el tractament de dades personals dels treballadors

En compliment de l'obligació d'informar derivada de l'article 13 del Reglament (UE) 2016/679, Reglament General de Protecció de Dades (RGPD) i LO 3/2018, de 5 de desembre, de Protecció de Dades Personals, CÀRITAS MATARÓ et facilita la següent informació relativa al tractament de les teves dades personals.

Qui és responsable del tractament de les teves dades personals?

CÀRITAS INTERPARROQUIAL MATARÓ amb NIF R0800544I

Carrer L'explanada, 72, 08301 Mataró. Correu-e: cim@caritasmataro.org

Contacte Delegat Protecció Dades: PROFESSIONAL GROUP CONVERSIA SLU

Per a què tractem les teves dades personals?

Amb la finalitat de realitzar tots aquells tràmits administratius, fiscals i comptables necessaris per a complir tant els nostres compromisos contractuals com les nostres obligacions legals en matèria laboral, Seguretat Social, prevenció de riscos laborals, fiscal i comptable, incloent concretament:

- Gestió de retribucions salarials, incloent-hi el de pagament de nòmines mitjançant entitat financera.
- Gestió d'expedient laboral (permisos, baixes, vacances, sancions, etc.)
- Control horari a través del sistema de control d'accés mitjançant l'aplicatiu INTRATIME .
- Dins dels límits legalment establerts, control laboral de l'activitat duta a terme mitjançant els equips i dispositius electrònics de CÀRITAS MATARÓ posats a la disposició del treballador.
- Gestió de les assegurances col·lectives de CÀRITAS MATARÓ

- Gestió d'accions formatives.
- Gestió de processos de promoció interna.
- En cas de disposar del teu consentiment exprés, publicació de la teva imatge en l'àmbit d'accions promocionals de l'activitat de CÀRITAS MATARÓ a través del lloc web corporatiu, perfil corporatiu de Càritas en xarxes socials, revista Càritas o un altre tipus de publicacions similars.

Quina és la legitimació per al tractament de les seves dades?

Les teves dades personals seran tractades amb les següents bases legals de legitimació:

- Necessitat per a l'adequada execució del contracte laboral que et vincula amb CÀRITAS MATARÓ (art. 6.1.b) RGPD).
- Compliment d'obligacions legals (art. 6.1.c) RGPD) derivades, entre altres, de les següents normes:
  - Reial decret legislatiu 2/2015, de 23 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut dels Treballadors.
  - Llei 31/1995, de 8 de novembre de Prevenció de Riscos Laborals
  - Llei General de la Seguretat Social.
  - Llei 42/1997, de 14 novembre, reguladora de la Inspecció de Treball.
  - Llei General Tributària.
- Existència de consentiment exprés (art. 6.1 a) RGPD) en relació amb la utilització de la imatge del treballador amb finalitats promocionals.

Durant quant temps conservarem les seves dades personals?

Les dades personals tractades en l'àmbit d'execució del contracte de treball que et vincula amb CÀRITAS MATARÓ seran conservades mentre duri la relació laboral i, en finalitzar la mateixa per qualsevol causa, seran conservades durant el termini de sis anys transcorregut el qual les dades seran suprimides, tret que subsisteixi la necessitat de conservar-les per motius legals.

L'interessat podrà revocar en qualsevol moment el consentiment atorgat pel tractament de dades personals que requereixin d'aquest, com per exemple l'ús de la teva imatge amb finalitats promocionals. No obstant això, la retirada del consentiment no afectarà la licitud del tractament basat en el consentiment previ a la revocació.

Com obtenim les teves dades de caràcter personal?

Directament de tu, com a interessat/da

A qui podem facilitar les teves dades?

Quan legalment procedeixi, les teves dades personals es podran facilitar a les categories de destinataris que es detallen a continuació:

- Prestadors de serveis auxiliars externs vinculats a CÀRITAS MATARÓ com a Encarregats de Tractament, com ara gestories laborals, assessories jurídiques, entitats financeres, prestadors de serveis de IT amb accés a dades personals com serveis de ciberseguretat, suport informàtic, hosting i altres similars.
- A entitats privades i Administracions Públiques finançadores d'activitats de CÀRITAS MATARÓ mitjançant subvencions.
- A l'Agència Tributària.
- Organismes de la Seguretat Social, Mútua d'Accidents de Treball i Malalties Professionals de la Seguretat Social.
- Inspecció de Treball

- Jutjats i Tribunals de Justícia.
- Entitats que participin en la gestió de cursos de formació als quals desitgi assistir el treballador amb la finalitat de participar en els cursos que s'organitzin.
- Sindicat en cas que procedeixi per al descompte de la quota obrera.
- Empreses de rènting o lloguer de vehicles per a ús dels treballadors, reserves en hotels i mitjans de transport públic.

Com protegirem les teves dades personals?

El tractament de les teves dades personals es durà a terme adoptant les mesures de seguretat física, lògica i organitzativa necessàries per a evitar la pèrdua, ús indegut, alteració i accés no autoritzat a aquests, tenint en compte l'estat de la tecnologia, la naturalesa de les dades i l'anàlisi de riscos efectuat.

Quins són els teus drets en matèria de protecció de dades personals com a interessat?

Els drets legalment establerts en matèria de protecció de dades personals són: drets d'accés, rectificació, supressió, oposició, limitació, portabilitat i no sotmetiment a decisions individuals automatitzades.

Per a exercir els esmentats drets podràs formular la teva petició per escrit i dirigir-la per correu postal o electrònic a dpd.cliente@conversia.com

En el cas que consideris que els teus drets en matèria de protecció de dades personals no han estat adequadament atesos, podràs presentar una reclamació davant l'Agència Espanyola de Protecció de Dades.

En el cas de produir-se alguna modificació de les teves dades, t'agraïm que ens el comuniquis degudament per escrit amb la finalitat de mantenir les teves dades actualitzades.

Seran les teves dades objecte de transferències internacionals a tercers països no inclosos en l'Espai Econòmic Europeu?

CÀRITAS MATARÓ no té previst realitzar transferències internacionals de dades.

Avís informatiu sobre el tractament de dades personals dels voluntaris

Qui és responsable del tractament de les teves dades personals?

CÀRITAS INTERPARROQUIAL MATARÓ

El seu domicili és C/ L'Esplanada 72,08301 Mataró.

Correu electrònic Càritas de Mataró: cim@caritasmataro.org

Contacte Delegat de Protecció de Dades CÀRITAS MATARÓ: dpd.cliente@conversia.es o trucant al telèfon 902 877 192.

Per a què tractem les teves dades personals?

Per a complir la nostra missió: promoure el desenvolupament integral de les persones i els pobles, especialment dels més pobres i exclosos. Com a persona voluntària, amb la finalitat de gestionar la teva col·laboració.

Les teves dades seran conservades durant 10 anys una vegada finalitzada la teva col·laboració.

En el teu procés d'incorporació a Càritas, necessitem determinar la teva adequació al perfil per a cada activitat o funcions que vagis a exercir. En funció de la col·laboració que estableixis amb

Càritas, les teves dades es podran utilitzar per a establir o realitzar perfils o estudis de realitats i situacions socials.

Quines dades personals tractem?

Càritas recull les teves dades identificatives personals (nom, cognoms, DNI, domicili, telèfon), així com el teu recorregut formatiu i laboral.

Com obtenim les teves dades de caràcter personal?

Tens obligació de facilitar-nos les teves dades per a poder col·laborar amb nosaltres.

Les teves dades són recollides pels casos d'obligació legal davant Administracions Públiques, per la Llei 38/2003 General de Subvencions, i per la relació contractual de l'acord d'incorporació establert per la Llei 025/2015 de 30 juliol de2015 del Voluntariat.

A qui podem facilitar les teves dades?

Les teves dades estaran a la disposició de Càritas de Mataró per a activitats formatives, amb motiu d'auditoria interna o externa, per a participar, en el seu cas, en els processos de gestió i en la presa de decisions de Càritas, així com en l'elaboració, disseny, execució i avaluació dels programes en què puguis intervenir.

Les teves dades seran comunicades a les companyies asseguradores a l'efecte de concertar les pòlisses legalment exigides.

En funció del projecte en el qual participis, les teves dades podran ser cedides a Administracions Públiques, empreses d'inserció vinculades a Càritas i finançadors privats dels projectes de Càritas.

Càritas garanteix que no facilitarà les teves dades a tercers sense el teu consentiment, excepte en els supòsits assenyalats anteriorment i en els legalment establerts.

Càritas no realitza transferències internacionals de dades.

Quins són els teus Drets?

Pots exercitar els drets d'accés, rectificació, supressió i portabilitat de les teves dades, i la limitació o oposició al seu tractament a través de les adreces postals i electròniques indicades en aquest document.

Així mateix si consideres que el tractament de les teves dades personals vulnera la normativa o els teus drets de privacitat pots presentar una reclamació a:

- Delegat de Protecció de Dades de Càritas Mataró a través de la seva adreça postal o electrònica,
- Delegat de Protecció de Dades de CÀRITAS MATARÓ a través de la seva adreça postal o electrònica.

  També tens dret a reclamar davant l'Autoritat de Control:

- Agència Espanyola de Protecció de Dades a través de la seva seu electrònica https://www.agpd.es/ o adreça postal.

7. CONSEQÜÈNCIES DE L'INCOMPLIMENT DEL PRESENT MANUAL

L'agent s'obliga expressament a complir les polítiques, normes, mesures, procediments, regles i estàndards que s'especifiquen en el present document. CÀRITAS INTERPARROQUIAL MATARÓ

podrà contemplar en el seu règim sancionador les mesures a aplicar relacionats amb els incompliments deliberats o per negligència de les obligacions contemplades en aquest manual.

8. ACCEPTACIÓ

Com a usuari manifest que conec el contingut del present Manual i accepto les polítiques i normes exposades en aquest, comprometent-me al seu compliment.

Qualsevol canvi substancial del present document serà comunicat per escrit a tots els usuaris, ja sigui a través del servei de correu electrònic o mitjançant un altre instrument de comunicació interna habilitat a aquest efecte.

(NOTA: Mitjançant la signatura d'aquest document, l'usuari agent de Càritas expressa la seva acceptació a les polítiques i normes contingudes en el Manual de Seguretat de l'Agent enunciada en aquest apartat 8).

A Mataró, ... de .....de 20

Signatura

.....

Nom complert:.....

ANNEX 1

APLICACIONS WEB I MÒBILS DE CARITASMATARO.ORG AMB TRACTAMENT DE DADES PERSONALS

Les aplicacions disponibles en els Sistemes d'Informació de CÀRITAS INTERPARROQUIAL MATARÓ són les que es recullen en el document Aplicacions Web de caritasmataro.org

RECOMANACIONS COMPLEMENTÀRIES PER A LA SEGURETAT DE LA INFORMACIÓ

D'acord amb la Política de Seguretat de la Informació, es desplega seguidament una sèrie de criteris d'ús diligent i bones pràctiques dels sistemes d'informació, amb la finalitat d'ajudar la protecció de les dades personals i prevenir riscos i amenaces que generin incidències en els sistemes d'informació, que poden ser intencionals o accidentals, procedents de fora o, fins i tot, de dins de l'organització i que poden arribar a perjudicar la reputació de Càritas. Alguns d'aquests criteris es deriven del Codi de Conducta de CÀRITAS MATARÓ amb la finalitat d'evitar comportaments incompatibles amb els valors de l'organització. Aquests criteris s'estructuren entorn de quatre apartats rellevants:

- Altres dispositius.
- Internet.
- Correu electrònic.
- Informació en paper.

Criteris per a l'ús d'altres dispositius.

Pantalles netes

Cada agent serà responsable del seu lloc i procurarà evitar que cap persona accedeixi a la informació que està sota la seva responsabilitat sense la deguda autorització.

Tots els equips tenen configurat un protector de pantalla que impedeix la visualització de les dades. La represa del treball implicarà la desactivació del protector mitjançant la introducció de la contrasenya. Tots els agents han de bloquejar manualment els seus equips quan abandonin momentàniament el lloc de treball (Tecla Windows+ tecla L premudes alhora), especialment si consideren que pot existir perill per a la confidencialitat de la informació que estan manejant en aquell moment, sobre tot, per a les dades de caràcter personal.

En resum, s'han de tancar tots els arxius amb informació confidencial i bloquejar l'equip abans d'abandonar el lloc de treball.

Compartir escriptori

En determinats casos, i només quan així hagi estat específicament aprovat per cada responsable d'àrea, un agent podrà compartir el seu escriptori per a ser visualitzat o fins i tot administrat remotament amb aplicacions com Teamviewer, etc. En aquests casos, s'estableixen les següents regles de seguretat, que no s' apliquen quan és l'Equip de Gestió de la Informació qui fa aquests treballs:

- L'agent haurà de ser present i atent a les accions realitzades pel gestor remot, en cap concepte es deixarà l'equip desatès.
- Totes les aplicacions hauran de ser tancades, a excepció de les necessàries per a mantenir la comunicació o sessió de suport.
- Haurà d'assegurar-se que no existeixen fitxers visibles en l'escriptori.
- No es podrà efectuar transferència de fitxers en l'aplicació d'escriptori compartit.
- L'equip no podrà ser gestionat sense consentiment exprés de l'agent usuari.
- Haurà d'assegurar-se que l'aplicació i sessió queden tancades una vegada finalitzada la sessió de suport.
- Haurà d'assegurar-se que la contrasenya de l'equip compleixi amb les mesures de seguretat de contrasenyes que s'indiquen en l'apartat "Gestió de contrasenyes"

Viatges amb els PC

En cas d'haver de viatjar amb l'equip, mai es facturarà aquest amb l'equipatge, excepte si la normativa legal ho exigís.

La pèrdua o robatori del dispositiu informàtic portàtil ha de ser notificada immediatament a l'Equip de Gestió de la Informació i Gestió d'incidències.

Seran responsabilitat de l'agent:

- Els desperfectes ocasionats a conseqüència del seu trasllat en dispositius no adequats (bosses, maletes, etc.).
- Els desperfectes ocasionats a conseqüència d'un ús inadequat.
- La pèrdua per oblit en llocs públics.

Verificacions

Per a verificar el compliment de les normes del present Manual, així com el correcte funcionament de l'equip i el bon ús d'aquest, es realitzaran verificacions per part del Responsable de Seguretat de la Informació de CÀRITAS MATARÓ, dels equips dels agents a fi d'examinar aspectes com:

- Aplicacions instal·lades i registre del sistema operatiu.
- Estat de l'antivirus.

Aquestes revisions podran ser manuals o automàtiques mitjançant algun programari de control. Les mateixes consideracions s'apliquen respecte dels equips de sobretaula.

Una vegada examinat l'equip de l'agent, el contingut no autoritzat podrà ser eliminat, i l'agent serà informat de les seves obligacions respecte de l'equip, i de les conseqüències del no respecte d'aquestes directrius.

Els equips seran lliurats a l'agent en perfecte estat i funcionament. Si l'agent detectés algun desperfecte, mal funcionament o contingut indegut en rebre l'equip, haurà de posar-lo immediatament en coneixement del seu Coordinador d'Equip, amb la finalitat que es pugui solucionar l'incident.

Software de virtualització

Els agents que requereixin tenir instal·lat algun Software de virtualització[2] de màquines, com VirtualBox, HyperV, VMWare, etc., el sol·licitaran a través del seu responsable, indicant quines màquines virtuals necessitaran, per a quina finalitat i quins requeriments tindran (sistema operatiu, configuració de xarxa, emmagatzematge, etc.). Una vegada instal·lat el programari i les màquines virtuals requerides, si té noves necessitats les haurà de sol·licitar a l'Equip de Gestió de la Informació.

Ús responsable de mòbil, telèfon

CÀRITAS INTERPARROQUIAL MATARÓ proporciona accés i ús de les comunicacions telefòniques per al millor acompliment de les seves activitats. L'ús inadequat d'aquests dispositius, pot perjudicar tant la integritat de les dades personals com la imatge i els fins de CÀRITAS INTERPARROQUIAL MATARÓ. Això pot esdevenir mitjançant la realització d'activitats considerades il·lícites que atemptin contra la moral o puguin resultar ofensives o mitjançant l'ús abusiu d'aquest.

a) Telèfon mòbil

En cas de tractar-se de terminal i contracte corporatiu de CÀRITAS INTERPARROQUIAL MATARÓ, l'agent queda informat que s'hi pot instal·lar una eina de gestió de la seguretat d'aquest dispositiu, que podrà realitzar accions com les següents, amb l'objectiu únic de protegir la informació amb dades de caràcter personal accessible des del terminal (correu, contactes, etc.) davant casos de pèrdua o robatori:

- Limitació d'aplicacions a instal·lar.
- Limitació de xarxes de connexió.
- Geolocalització de dispositiu en temps real, d'acord amb els límits establerts per la legislació vigent.
- Accés al llistat de crides.
- Gestió remota del dispositiu.
- Esborrat remot del dispositiu.
- Xifratge del dispositiu.
- Etc…

L'agent haurà de protegir la informació de CÀRITAS MATARÓ que pogués estar continguda en els terminals, tant si es tracta d'aparells corporatius de la institució com si són personals.

Les mesures mínimes de seguretat que hauran d'establir-se són:

- Protegir el dispositiu amb un número PIN d'almenys 4 caràcters, patró de 4 punts o empremta dactilar (en funció del que permeti el terminal).
- Evitar que aquest mètode d'accés pugui ser conegut per altres persones.
- Evitar la connexió a xarxes sense fils (WIFI) desconegudes.
- Evitar la instal·lació d'aplicacions provinents de fonts desconegudes o insegures.

[2] *Software de virtualització: programari que permet simular l'existència de maquinari i permet crear un sistema informàtic virtual o màquines virtuals. Permet executar més d'un sistema virtual sobre el mateix sistema real agent no podrà afegir noves màquines virtuals ni podrà modificar la configuració de cap d'elles, tampoc instal·lar cap programari addicional, encara que tingui drets per a això.*

- Evitar la manipulació del sistema operatiu subministrat en el terminal, fora dels procediments homologats d'actualització.
- En terminals mòbils o línies telefòniques de la institució, evitar l'enviament d'acudits, memes, comentaris o imatges que continguin insults, epítets racials o qualsevol altra expressió que pogués ofendre, denigrar o avergonyir a uns altres, especialment sobre la base de motius de raça, nacionalitat, gènere, orientació sexual, edat, discapacitat, religió, creences polítiques o altres raons a les quals el destinatari pugui ser sensible mitjançant l'ús de plataformes de missatgeria instantània tipus (Whatsapp, Telegram…).
- No és recomanable usar ni enviar les teves dades personals a través de plataformes de missatgeria instantània (Whatsapp, Telegram, Signal…) i queda expressament prohibit l'enviament de dades personals preses o registrats en Càritas mitjançant aplicacions com són les de beneficiaris, donants, etc. o fotos d'agents de Càritas o de tercers en primer pla.

CÀRITAS INTERPARROQUIAL MATARÓ proporciona un MDM3 per als seus terminals corporatius.

3 MDM: de l'original en anglès, “Mobile Device Management”, Gestió de Dispositius Mòbils

La pèrdua o robatori del dispositiu ha de ser notificada immediatament a través dels mitjans anteriorment definits.

Dispositius telefònics

L'ús personal de les comunicacions a través de dispositius corporatius es pot efectuar mentre no interfereixi amb les activitats laborals habituals. Qualsevol ús personal:

- No ha de comportar un cost que superi un llindar raonable.
- No ha de tenir caràcter comercial.
- No ha de posar en risc la reputació i el nom de CÀRITAS MATARÓ.
- No ha de suposar comportament antisocial o immoral.
- No ha de ser incompatible amb els valors propis de Càritas.
- No ha de servir per a la divulgació no autoritzada d'informació confidencial de CÀRITAS MATARÓ.
- No ha de contravenir l'ordenament jurídic.
- No ha d'estar associat a una entitat política.

L'accés dels agents a aquest accés ha de limitar-se als necessaris per a dur a terme les labors corresponents a les seves tasques.

No està permès l’ús de les comunicacions telefòniques de CÀRITAS MATARÓ per a transmetre o distribuir missatges o continguts inapropiats, violents, ofensius o discriminatoris.

Els usuaris de les comunicacions telefòniques de CÀRITAS MATARÓ no hauran de fer-se passar per un altre usuari o entitat en el transcurs de qualsevol comunicació.

CÀRITAS MATARÓ es reserva el dret de revisar la llista de crides realitzades, per a la verificació del compliment de les normes davant qualsevol sospita o evidència d'ús fraudulent o abusiu d'aquest.

Ús responsable d'internet

L'ús d'Internet en l'àmbit de CÀRITAS MATARÓ té caràcter fonamentalment laboral; no obstant això -amb l'objectiu de facilitar la conciliació de la vida laboral, familiar i personal- es permetrà l'ús moderat, raonable i responsable d'Internet amb finalitats particulars, sense perjudici de la lícita facultat de vigilància i control per l'entitat. Aquest ús particular es realitzarà sempre amb el màxim respecte a la llei i a l'ètica, i de manera que no es vegi perjudicat el rendiment ni les tasques del treballador. En qualsevol cas, els agents són els únics responsables de les sessions iniciades en la xarxa Internet des de les seves terminals de treball.

Directrius per a l'ús d'internet

- En cap cas es poden modificar les configuracions dels navegadors[3] de l'equip ni l'activació de servidors o ports sense autorització del Responsable de Seguretat de CÀRITAS MATARÓ.
- En particular, encara que no es limiti tècnicament la capacitat ha de limitar-se la utilització d'imatges (com els formats *GIF, *JPG, *BMP o *TIFF entre altres), so (formats *WAV i MP3 principalment) i vídeo (*MPG, *DivX, *AVI, *RAW o similars) per a fins aliens a l'activitat laboral de l'entitat, pel fet que la grandària d'aquests arxius satura els canals de comunicació i disminueix la velocitat de transmissió perjudicant el funcionament de la xarxa en el seu conjunt.
- Sempre que sigui possible, es preferirà l'accés a llocs d'Internet que comptin amb mesures de seguretat addicionals, com per exemple el xifratge de la informació en trànsit mitjançant HTTPS (l'adreça d'Internet tindrà la forma https://).
- No es permetrà l'emmagatzematge d'informació de CÀRITAS MATARÓ en eines d'emmagatzematge en el núvol[4].
- En cap cas es podran rebre o descarregar arxius o informació que contingui dades de caràcter personal sense tenir en consideració el que es preveu en l'apartat d'aquest Manual relatiu a Protecció de Dades de Caràcter Personal.
- Els agents hauran d'observar, abans de la utilització de qualsevol informació obtinguda d'Internet, si l'ús d'aquesta informació està restringit per les lleis que protegeixen la propietat intel·lectual o industrial. En particular, quant a programes informàtics descarregats des d'Internet, hauran d'observar-se les pautes descrites en l'apartat sobre "Descàrrega de material subjecte a drets d'autor".
- No està permès l'ús d'Internet amb propòsits il·legals, inapropiats o obscens, i que ofenguin la moral. Dins de l'ús inapropiat es troba canviar el propòsit i la finalitat de l'ús d'Internet i de les xarxes de comunicació en l'àmbit laboral.
- Així mateix, no es podrà emprar Internet o la web mitjançant els recursos informàtics o de xarxa de CÀRITAS MATARÓ amb finalitats recreatives, així com per a obtenir o distribuir material violent, pornogràfic de qualsevol altra índole que sigui incompatible amb els valors de CÀRITAS MATARÓ.
- No està permès l'accés, la descàrrega i/o l'emmagatzematge en qualsevol suport, de pàgines o continguts il·legals, inadequats o que atemptin contra la moral i els bons costums; dels formats d'imatges, sons o vídeo que a tall d'exemple s'enumeren en la norma anterior; de virus i codis maliciosos i, en general, de tota mena de

[3] *Navegador: programari instal·lat en l'ordinador que permet l'accés als llocs web perquè aquests puguin ser visualitzats. Exemples: Firefox, Google Chrome, Internet Explorer, etc.*

[4] *Emmagatzematge en el núvol: model d'emmagatzematge de dades en sistemes aportats per tercers i que són accessibles a través d'Internet*

programes i/o plugins sense l'expressa autorització del Responsable de Seguretat de CÀRITAS MATARÓ.

- CÀRITAS MATARÓ es reserva el dret a filtrar i limitar el contingut al qual l'agent pugui accedir a Internet per mitjà de l'ús dels seus recursos i serveis en el cas de seguiment de recerca de qualsevol activitat sospitosa, il·lícita o delictiva, així com registrar els accessos realitzats des de l'equip. D'acord amb els límits determinats en la normativa aplicable, podrà monitorar en el seu cas, l'ús inadequat d'Internet al marge de l'acompliment laboral.

Accés des d'equips no corporatius

Cal establir protocols segurs per poder accedir a les dades des de dintre i des de fora de les seus. S'ha subministrat el programari i la configuració personal per a tal efecte, però cal extremar al màxim les mesures de seguretat als dispositius no corporatius.

L'ordinador haurà de disposar un perfil específic amb contrasenya per accedir al programari que permeti accedir a les dades de Càritas. La contrasenya haurà de seguir els criteris establert per als dispositius corporatius de Càritas.

S'haurà d'evitar que altres usuaris del mateixos dispositius puguin concedir-se permisos per tal d'evitar la possibilitat d'accés a les dades.

Els dispositius hauran d'estar xifrats tal com s'indica en els dispositius propis de Càritas.

No es podrà fer servir cap programari "pirata" als dispositius que tinguin accés a les dades de feina. En cas necessari, Càritas podrà instal·lar el programari i les llicències indispensable per treballar amb les dades (Windows, Office, SSHFS,...)

S'instal·larà el programari subministrat per l'asseguradora per tal d'evitar i/o controlar que puguin accedir a les dades de Càritas.

Durant el treball amb les dades de Càritas s'hauran de seguir els mateixos criteris que per als dispositius de Càritas:

- Es treballarà directament a la unitat de dades CIM
- No es faran copies temporals al Dispositiu. Si per alguna raó es fan, s'hauran de desar a la carpeta corresponent de les dades CIM i esborrar-les de l'escriptori, documents, etc.
- Es bloquejarà la pantalla o, millor, es tancarà la sessió quan no s'estigui treballant amb les dades de Càritas.

En resum, es mantindran al màxim els mateixos criteris que als dispositius corporatius de Càritas.

Descàrrega de material subjecte a drets d'autor

Per motius de seguretat, no està permesa la descàrrega de programari executable des d'Internet. L'Equip de Gestió de la Informació serà l'únic que podrà realitzar aquestes descàrregues. D'igual manera, en cap cas podrà descarregar-se programari ni continguts protegits per drets de propietat intel·lectual i/o industrial amb la finalitat d'utilitzar-ho i/o distribuir-ho posteriorment pels recursos informàtics i de xarxa de CÀRITAS MATARÓ sense la corresponent llicència d'ús i/o distribució d'aquest material. Davant aquesta mena de necessitats, l'agent es dirigirà al seu Coordinador d'Equip amb la finalitat de realitzar l'oportuna sol·licitud al Responsable de Seguretat.

Els agents respectaran i donaran compliment a les disposicions legals sobre propietat intel·lectual i/o industrial en relació amb qualsevol informació visualitzada o obtinguda mitjançant Internet fent ús dels recursos informàtics o de xarxa corporatius.

En cap concepte es cometran infraccions o transgressions contra els drets de propietat intel·lectual o industrial, per exemple, instal·lant o distribuint programari "pirata" o utilitzant imatges, música, textos o altres obres de propietat intel·lectual sense la deguda autorització del titular dels drets.

Consideracions de privacitat en l'ús d'internet

Els agents respectaran en tot moment la privacitat aliena en l'àmbit d'Internet. En aquest sentit, no buscaran ni faran ús o s'apoderaran d'informació personal aliena, ni obtindran còpies del programari, arxius, dades ni contrasenyes pertanyents a altres usuaris d'Internet. No duran a terme voluntàriament conductes de suplantació d'identitat d'un altre agent o usuari.

Els agents no modificaran ni eliminaran el programari, els arxius, dades ni contrasenyes d'altres usuaris o agents intencionadament, excepte autorització expressa d'aquests usuaris. Es requereix que els agents respectin la integritat de la informació pertanyent a altres usuaris que fan ús d'Internet.

S'haurà d'obtenir els permisos necessaris per a obtenir informació personal o altres recursos d'Internet que no siguin de lliure accés al públic. No es permetran els intents d'accedir a la informació privada o altres recursos d'Internet sense haver obtingut l'aprovació adequada.

Ús responsable del correu electrònic

El correu electrònic ("e-mail") és una eina útil per enviar i rebre missatges, obtenir i enviar informació i establir relacions d'intercanvi per a l'activitat. No obstant això, tret que sigui usat apropiadament, pot crear problemes de seguretat i de responsabilitat legal per a CÀRITAS MATARÓ. Per això, aquestes Normes d'ús de correu electrònic tenen com a objectiu afavorir la protecció dels actius i les dades personals de l'entitat i reduir la seva possible responsabilitat legal.

El servei de correu electrònic

El servei de correu electrònic corporatiu, la titularitat del qual correspon a CÀRITAS MATARÓ, es posa a la disposició dels agents mitjançant comptes personals de correu electrònic per treballar exclusivament en l'àmbit de les activitats pròpies de CÀRITAS MATARÓ. Per tant, s'evitarà l'ús del correu electrònic corporatiu amb finalitats extra laborals.

CÀRITAS MATARÓ podrà exercir les facultats de tutela i vigilància en relació amb el compliment de les obligacions relatives a l'ús del correu electrònic de Càritas sobre la base d'un triple criteri de necessitat, idoneïtat i proporcionalitat, d'acord amb la legalitat i amb fi de prevenir responsabilitats –incloent responsabilitats penals- derivades de l'ús indegut del correu electrònic, així com per a garantir la seguretat del sistema d'informació i la protecció de les dades personals.

Ús del correu electrònic

L'accés i ús d'aquest servei per part dels agents, han de limitar-se al que resulti adequat en l'exercici de les seves funcions, i en cas d'ús indegut, hauran de respondre de totes les activitats realitzades mitjançant ell.

Els missatges de correu transmeten informació en les seves capçaleres (en principi ocultes) que indiquen dades addicionals de l'emissor, per la qual cosa han de tenir-se en compte possibles repercussions (com a danys a la imatge institucional) que podria implicar una mala utilització d'aquest recurs.

El sistema informàtic de CÀRITAS MATARÓ inclou protecció antivirus. No obstant això, els usuaris han d'abstenir-se d'enviar o obrir missatges que resultin sospitosos, havent de comunicar qualsevol anomalia que observin a l'Equip de Gestió de la Informació.

No està permès l'enviament de comunicacions comercials no sol·licitades (spam) sense haver obtingut el degut consentiment.

L'agent haurà d'actuar amb discreció en enviar correu electrònic a "tots els usuaris" del sistema de Càritas, o a qualsevol altra llista gran de destinataris, ja sigui interna o externa, utilitzant el camp de CCo (còpia oculta) destinat a aquest efecte.

Amb caràcter general, l'agent evitarà l'enviament de dades personals de categoria especial (especialment sensibles) mitjançant correu electrònic. En cas de ser necessari tal enviament, les dades hauran de ser xifrades.

Quan s'estableixi la necessitat de xifrar o signar electrònicament els correus electrònics intercanviats amb un proveïdor o qualsevol altre tercer, el Coordinador de l'Equip de l'agent interessat consultarà amb el Responsable de Seguretat de la Informació els mecanismes disposats per CÀRITAS MATARÓ per a aquesta mena d'operacions.

No es podran realitzar cap de les següents activitats:

- Participar en la propagació de cartes encadenades, esquemes piramidals o similars.
- Distribuir missatges amb continguts inapropiats per a l'entitat.
- Falsificar les capçaleres del correu electrònic.
- Difondre missatges d'assetjament, denigrants, discriminatoris, ofensius o violents.
- Difondre acudits, comentaris o imatges que puguin resultar ofensius o denigrants per raons de discriminació racial, origen nacional, sexe, orientació sexual, edat, discapacitat, religió, creences polítiques o altres raons semblants a les que el destinatari pugui ser sensible.
- Enviar missatges a través de comptes aliens sense consentiment del seu titular.
- Permetre la utilització del compte corporatiu de correu electrònic i/o la corresponent bústia a persones no autoritzades.
- Efectuar accions a fi d'impossibilitar o obstruir sistemes informàtics (atacs de denegació de servei), dirigit a un usuari o al propi sistema de correu, així com l'enviament d'un nombre alt de missatges per segon (mail bombing), o qualsevol variant, que tingui per objecte la paralització del servei per saturació de les línies, de la capacitat de CPU del servidor, de l'espai en disc de servidors o terminals o qualsevol altra pràctica similar.
- Enviar missatges que comprometin la reputació de CÀRITAS INTERPARROQUIAL MATARÓ a fòrums de discussió, llistes de distribució i/o newsgroups.
- Reexpedir automàticament missatges (autoforwarding) de correu electrònic a adreces que no siguin de CÀRITAS INTERPARROQUIAL MATARÓ.
- Divulgar sense autorització documents confidencials de CÀRITAS INTERPARROQUIAL MATARÓ o enviar-los a destinataris no autoritzats.

- Enviar missatges i arxius que impliquin la vulneració de drets de propietat intel·lectual i/ o industrial corresponents a CÀRITAS INTERPARROQUIAL MATARÓ o tercers titulars.
- Fer ús del sistema de manera que causi congestió de la xarxa o ruptures de seguretat, com ara:
    - descàrrega d'arxius de grandària excessiva,
    - permetre-li a personal no autoritzat que usi el sistema, o
    - subscriure's a servidors de llistes o llistes de correu electrònic per a activitats no relacionades amb CÀRITAS INTERPARROQUIAL MATARÓ.

Informació impresa

Escriptoris nets

De la mateixa manera que s'exposava en l'apartat de Pantalles netes, cada agent serà responsable del seu lloc i procurarà evitar que cap persona accedeixi a la informació en paper que està sota la seva responsabilitat sense la deguda autorització.

Tots els usuaris han de seguir les següents normes sobre la informació impresa en paper:

- **Informació Confidencial**[5]
    - Ha de ser retornada sempre al seu lloc d'emmagatzematge quan s'acabi d'usar, no deixant cap documentació confidencial damunt de l'escriptori sense atenció. En cas que es realitzin fotocòpies/escanejat de documents, s'ha de retirar immediatament del dispositiu corresponent, retornant-lo al seu lloc d'emmagatzematge sota clau.
- **Informació d'ús intern**[6] **o pública**[7]
    - No existeixen consideracions especials, encara que sempre es vetllarà per la seguretat de la informació d'ús intern si existeixen persones alienes a l'organització, en les instal·lacions de l'empresa, mitjançant el bloqueig d'equips desatesos.

Les taules de treball dels usuaris han d'estar netes i ordenades, i en cap cas han de quedar sobre elles documents que continguin informació confidencial, incloent-hi dades personals. Tot suport d'informació que temporalment estigui fent servir un usuari ha de retornar-se al seu lloc

[5] *Informació que conté dades de caràcter personal de categoria especial, dades de donants o proveïdors de coneixement no públic, o documentació a la qual únicament té accés els òrgans de govern i en cas de divulgació pot causar perjudici a l'organització.*

[6] *Aquella informació disponible al personal de Càritas per a l'acompliment de les seves funcions (procediment, manuals, instruccions del sistema de gestió, etc.), i que no ha estat classificada com a confidencial o pública.*

[7] *Informació pública:*

- *Informació provinent de pàgines web, fullets publicitaris, presentacions, etc.*
- *Informació disponible en la web de Càritas atenint-se al que s'estableix per la Llei 19/2013 de Transparència (*art.6 i *art.8)*
- *Informació de domini públic sense intervenció del treballador.*
- *Informació que abans de la seva divulgació estava en possessió legítima del treballador.*
- *Informació que, després d'haver estat divulgada, sigui legalment rebuda d'una tercera part sense restriccions de divulgació.*
- *La informació ha de ser posada a la disposició d'un Jutjat o Tribunal.*

d'emmagatzematge quan s'acabi el seu ús, o custodiar-la sota clau en la calaixera de la taula en els períodes d'absència temporal del lloc.

En cas d'imprimir informació confidencial, assegurar-se que s'envia a la impressora desitjada i, sempre que la impressora ho permeti, es recomana utilitzar el sistema de "còpia segura". Amb aquest sistema és necessari la introducció d'un codi perquè la impressora realitzi la impressió, d'aquesta manera evitem que una altra persona se'ns avanci i tingui accés a la informació.

Per als enviaments per correu postal, no s'utilitzarà el correu ordinari per a l'enviament d'informació confidencial, sinó que s'utilitzaran alternatives segures: correu certificat o missatgeria.

Ús de la impressora, fotocopiadora i escàner

Els recursos de reprografia, impressió i digitalització a Càritas són eines que generen unes despeses que seran assumits per CÀRITAS MATARÓ sempre que el seu ús respongui a necessitats reals del treball. Quan es detecti un ús excessiu i inadequat d'aquests recursos, CÀRITAS MATARÓ podrà adoptar les mesures oportunes per a evitar-lo.

En qualsevol cas, l'agent ha de recordar la Política de Medi ambient i el compromís que ha adoptat sobre aquest tema CÀRITAS MATARÓ, per la qual cosa haurà d'assimilar i fer propi aquest compromís.

En tot cas, l'agent s'assegurarà que no quedin documents impresos en la safata de sortida o retinguts en la cua d'impressió que continguin documents confidencials o bé dades personals com es deia en l'apartat "Dades personals extretes del SICCE", així com de retirar els documents conforme vagin sent impresos. Aquest mateix compromís s'exercirà respecte de l'escàner o altres dispositius d'anàloga funcionalitat.

Respecte a la informació escanejada, CÀRITAS MATARÓ vetllarà el seu funcionament respecte a l'ús inadequat d'informació confidencial i de dades personals.

Una vegada acabades les tasques per a les quals van ser impresos, els documents que continguin dades de caràcter personal hauran de destruir-se utilitzant els recursos que destina CÀRITAS MATARÓ per destruir el paper (trituradores, caixes tancades per dipositar els documents a destruir, etc.)

ANNEX 2

DOCUMENTS COMUNICACIÓ VIOLACIÓ DE SEGURETAT

MODELO DE COMUNICACIÓN DE LA VIOLACIÓN DE SEGURIDAD

(MOD-CINT1) **MODELO DE COMUNICACIÓN INTERNA**
ENTRADA: ..... DÍA: ..... MES: ..... AÑO: ..... HORA: .....
IDENTIFICACIÓN DEL EMPLEADO QUE REALIZA LA COMUNICACIÓN: Nombre y Apellidos: DNI/NIE: Cargo: 1. DESCRIPCIÓN DE DUDA, SUGERENCIA, COMUNICACIÓN: 2. COMUNICACIÓN DE VIOLACIÓN DE SEGURIDAD DE LOS DATOS PERSONALES 2.1.-Descripción de la violación producida: 2.2.- Describir las consecuencias probables de la violación de seguridad de los datos personales (en caso de conocerse): 3. RELACIÓN DE DOCUMENTACIÓN ADJUNTADA: 1.-..... 2.-..... 3.-..... 4. OTROS COMENTARIOS
Firma/sello del comunicante

MODELO DE COMUNICACIÓN DE LA RESOLUCIÓN ANTE LA VIOLACIÓN DE SEGURIDAD

(MOD-CINT2) **RESULTADOS DEL ANÁLISIS DE LA COMUNICACIÓN**
SALIDA: ..... DÍA: ..... MES: ..... AÑO: ..... HORA: .....
Nº COMUNICACIÓN: DIRIGIDO A: Nombre y Apellidos: DNI/NIE: Cargo: **1.** DATOS DE REFERENCIA DE LA COMUNICACIÓN **2.** CONCLUSIONES DEL ANÁLISIS DE LA OPERACIÓN **3.** ACCIONES EFECTUADAS
Firma del Responsable de Privacidad