MANUAL DE SEGURETAT DE LES DADES CARÀCTER PERSONAL

Rev. 2

QUADRE D'APROVACIONS

	REALITZAT	APROVAT
RESPONSABLE	Equip de gerència	Equip de gerència
SIGNATURA		

LLISTA DE REVISIONS

REV.	DATA	DESCRIPCIÓ
0	04/07/2019	Nova edició per adequació al RGPD
1	14/06/2022	Revisió general del document
2	02/05/2023	Revisió formularis i registres

ÍNDEX

1.- OBJECTE

Aquest document ha estat elaborat sota la responsabilitat de GEDI GESTIÓ I DISSENY SCCL (en endavant GEDI) per a donar resposta a la necessitat d'establir garanties de seguretat adequades contra el tractament no autoritzat o il·lícit, la pèrdua, la destrucció o el dany accidental de dades de caràcter personal tractades per l'organització, segons estableix:

- Reglament (UE) 2016/679, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que respecte al tractament de dades personals i a la lliura circulació d'aquestes dades. (en endavant RGPD)
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals

En aquest document i en els documents complementaris s'estableixen les mesures organitzatives i tècniques encaminades a assegurar la integritat i confidencialitat de les dades personals i a demostrar que aquestes mesures es porten a terme.

GEDI es compromet a implantar i actualitzar les mesures tècniques i organitzatives que es recullen en aquest Manual de Seguretat que és d'obligat compliment per part de tot el personal de l'organització.

Aquest document estarà a la disposició de tot el personal, per al seu coneixement i consulta mitjançant la sistemàtica de distribució de documentació prevista al sistema de gestió de qualitat.

2.- ABAST

El Manual de seguretat és d'aplicació a tots els tractaments de dades de caràcter personal que realitza GEDI, tant en la condició de responsable com d'encarregat, i que es descriuen a FP002/F3 "Registre d'activitats de tractaments".

Quan GEDI realitza el tractament de les dades com a encarregat, aquesta relació estarà establerta i documentada mitjançant contractes i/o convenis.

A partir de l'anàlisi de riscos dels tractaments de dades de caràcter personal es determina que GEDI realitza tractament de dades personal especialment sensibles i amb un nivell de risc alt per a als drets i llibertats de les persones interessades.

En l'Annex B es detalla la gestió de riscos dels tractaments que porta a terme GEDI per a determinar les mesures de seguretat del sistema de protecció de dades de caràcter personal.

3.- RECURSOS PROTEGITS

L'establiment de garanties de seguretat de les dades de caràcter personal es realitzarà mitjançant el control de totes les vies per les quals es pugui tenir accés a les mateixes i tenint en compte tot el cicle de vida de les dades a GEDI.

Els recursos directes o indirectes per accedir a les dades, que hauran de ser controlats són:

- Els centres de tractament i/o locals on es trobin les dades o s'emmagatzemin els suports que les continguin.
- L'entorn informàtic i de comunicacions.

- Aplicacions establerts per a accedir a les dades.

La descripció dels recursos protegits es detalla a l'Annex A i s'amplia per a cada servei mitjançant FP002/F7 "Recursos protegits per servei".

4.- MESURES ORGANITZATIVES

El personal afectat per la normativa establerta en aquest Manual es classifica en les següents funcions:

- **Administradors**, són encarregats d'administrar o mantenir l'entorn operatiu de les dades, és a dir, per les seves funcions poden utilitzar eines d'administració que permetin l'accés a les dades. Es pot consultar a FP002/F9 "Llista d'Administradors i Responsables de Seguretat" les persones que tenen assignada aquesta funció.

- **Responsable Seguretat Global (RSG)** equip nomenat per encarregar-se del manteniment, coordinació, seguiment i control del sistema de seguretat de les dades en l'àmbit general de l'organització. Estarà constituït pel Responsable de Qualitat i el Responsable d'Informàtica. Es pot consultar a FP002/F9 "Llista d'Administradors i Responsables de Seguretat" les persones que tenen assignada aquesta funció.

- **Responsable Seguretat Local (RSL)** persona nomenada per encarregar-se del manteniment, coordinació, seguiment i control del sistema de seguretat de les dades en l'àmbit d'un Servei. Es pot consultar a FP002/F9 "Llista d'Administradors i Responsables de Seguretat" les persones que tenen assignada aquesta funció.

- **Usuaris** persones treballadores que utilitzen el sistema informàtic d'accés a les dades o accedeix a les mateixes en suport paper. La consulta de les persones que tenen assignat aquesta funció es realitza mitjançant el control d'accessos al sistema informàtic.

Les principals funcions i obligacions de cadascuna d'aquestes funcions es detallen a l'Annex C.

Totes les persones amb accés a les dades personals han de tenir coneixement de les seves obligacions amb relació als tractaments de dades personals i seran informats sobre aquestes obligacions.

Per això, totes les persones han de signar el formulari FP002/F1 "Clàusula informativa i compromís de confidencialitat", abans d'accedir a les dades, aquest document conté la informació mínima que han de conèixer i se'ls informa de l'obligació de conèixer el "Manual de seguretat de les dades de caràcter personal", que estarà disponible per a la seva consulta per part de totes les persones treballadores a la web.

4.1. NORMES PER A TOT EL PERSONAL AMB ACCÉS A DADES PERSONALS

4.1.1. DEURE DE CONFIDENCIALITAT I SECRET

- Tractar les dades de caràcter personal d'acord amb les instruccions de GEDI establertes al Manual de Seguretat i que es distribueix d'acord al que estableix el sistema de gestió de la qualitat.

- No comunicar les dades a terceres persones, ni tan sols per a la seva conservació, llevat dels supòsits legalment admissibles o que compti amb l'autorització expressa de GEDI. Es tindrà especial cura en no facilitar dades personals protegides durant les consultes telefòniques, correus electrònics, etc. a excepció que s'estigui autoritzat.

- Protegir totes les dades tractades per GEDI; mantenir la confidencialitat i integritat de la informació, de les contrasenyes i del sistema informàtic/aplicacions a través de les quals s'hi accedeix; evitar la seva modificació o la seva destrucció quan no es té autorització.

- Aplicar tots els controls de seguretat necessaris per garantir la seguretat de la informació i de les dades en la prestació del servei. Sempre que s'introdueixin, modifiquin o eliminin dades de caràcter personal d'un fitxer s'haurà de confirmar que aquestes accions es fan tenint en compte les pautes establertes per GEDI.

- No extreure informació en cap format, tampoc mitjançant l'enviament telemàtic, si no es té l'autorització de GEDI.

- Evitar l'accés de persones no autoritzades a les dades personals, amb aquesta finalitat s'evitarà: deixar les dades personals exposades a tercers (pantalles desateses, documents en paper en zones d'accés públic, suports amb dades personals no custodiats, etc. .). Quan no s'estigui utilitzant l'equip, es procedirà al bloqueig de la pantalla o al tancament de la sessió. Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris o espais d'accés restringit). No es llençaran documents (informes, autoritzacions, expedients, ...) o suports electrònics (CDs, USB, discs durs, etc.) amb dades personals sense garantir-ne la seva destrucció.

- Utilitzar els recursos informàtics i de comunicació de GEDI amb l'única i exclusiva finalitat de prestar els serveis pels quals han estat previstos i no donar accés a la informació a persones no autoritzades.

- Els comptes de correu assignats són individuals i intransferibles i la persona usuària es compromet a utilitzar-los per a activitats que es troben únicament i directament relacionades amb el seu lloc de treball. L'ús del correu electrònic per a finalitats particulars està autoritzat, sempre que aquest ús es faci de forma moderada, no abusiva i en tot cas compatible amb l'ús primordial del mateix que és el desenvolupament de l'activitat assignada per GEDI.

- GEDI es reserva el dret de revisar, sense previ avís, els missatges de correu electrònic i els arxius LOG de la persona usuària de la xarxa corporativa, per identificar situacions irregulars o d'incompliment de les normativa establerta en matèria de seguretat amb la finalitat de prevenir activitats que puguin afectar-la com a responsable civil subsidiària.

- El deure de secret i confidencialitat persisteix fins i tot quan finalitzi la relació laboral de la persona treballadora amb GEDI.

4.1.2. DRETS DELS TITULARS DE LES DADES

Totes les persones treballadores han de facilitar que les persones interessades o els seus representants puguin exercir els drets sobre les seves dades de caràcter personal que tracta GEDI.

Amb aquesta finalitat, s'informarà a totes les persones treballadores del procediment per atendre els drets dels interessats, definint de forma clara els mecanismes pels quals es poden exercir (mitjans electrònics, adreça postal, etc.) i el procediment a seguir (Veure punt 8 d'aquest document).

És un requisit indispensable per exercir els drets sobre les dades de caràcter personal que la persona presenti un document acreditatiu de la seva identitat (document nacional d'identitat o passaport).

4.1.3. VIOLACIONS SEGURETAT DE DADES DE CARÀCTER PERSONAL

Quan es produeixin violacions de seguretat de dades de caràcter personal, com per exemple, el robatori o accés indegut a les dades personals s'ha de procedir a obrir una incidència i notificar-se a l'Agència Espanyola de Protecció de Dades en el termini de 72 hores. (Veure punt 6 d'aquest document).

5.- MESURES TÈCNIQUES

5.1. IDENTIFICACIÓ PERSONAL INEQUÍVOCA

- S'han de mantenir separats els usos professional i personal de l'ordinador. Per això, quan el mateix ordinador o dispositiu s'utilitzi per ambdós usos la/les unitat/s d'ús professional seran exclusivament per aquesta finalitat i no s'hi podran guardar dades d'ús personal. (consultar Annex A "Recursos protegits")

- Es disposarà de perfils amb drets d'administrador, per a la instal·lació i configuració del sistema, i perfils d'usuaris sense privilegis o drets d'administració per a l'accés a les dades personals. Aquesta mesura evitarà que en cas d'atac de ciberseguretat es puguin obtenir privilegis d'accés o modificar el sistema operatiu. (consultar FP002/F9 "Llista d'Administradors i Responsables de seguretat").

- Quan a les dades personals accedeixin diferents persones, per a cada persona amb accés a les dades personals, es disposarà d'un usuari i contrasenya específics (identificació inequívoca).

- S'ha de garantir l'existència de contrasenyes per a l'accés a les dades personals emmagatzemades en sistemes informàtics, les contrasenyes:
  - La contrasenya haurà de ser forta: ha de tenir com a mínim 8 caràcters i que figurin lletres majúscules, lletres minúscules, números i símbols; donant com a resultat una contrasenya que no contingui paraules o sèries numèriques obvies o fàcils d'endevinar.
  - Són confidencials, personals i intransferibles.

- Per assegurar la confidencialitat de les contrasenyes:
  - S'ha d'evitar que quedin exposades a tercers
  - En cap cas es compartiran ni es deixaran anotades en lloc comú i d'accés de persones diferents de l'usuari.
  - Es canviaran periòdicament, com a mínim anualment.
  - Si una persona coneix qualsevol situació que comprometi la confidencialitat de la contrasenya o l'ús fraudulent de la mateixa, haurà a comunicar-ho de forma immediata al **Responsable Seguretat Local (RSL)** per a procedir al seu registre a FP002/F5 "Notificació i registre d'incidència". (Consultar punt 6 "Gestió d'Incidències)

- Per a la gestió de les contrasenyes veure el que es descriu a l'Annex A "Recursos Protegits" i a FP002/F7 "Recursos protegits per servei".

5.2. DEURE DE SALVAGUARDA

Per a garantir la salvaguarda de les dades personals, a continuació s'exposen les mesures tècniques mínimes establertes.

- ACTUALITZACIÓ D'ORDINADORS I DISPOSITIUS: Els dispositius i ordinadors utilitzats per a l'emmagatzematge i el tractament de les dades personals es mantenen actualitzats en la mesura del possible, incloent versions dels sistemes operatius.

- ANTIVIRUS i MALWARE: En els ordinadors i dispositius on es realitzi el tractament automatitzat de les dades personals es disposarà d'un sistema d'antivirus que garanteixi en la mesura possible el robatori i destrucció de la informació i dades personals. El sistema d'antivirus són actualitzats de forma periòdica.

- TALLAFOCS O FIREWALL: Per evitar accessos remots indeguts a les dades personals es vetllarà per garantir l'existència d'un firewall activat en aquells sistemes, ordinadors i dispositius en els quals es realitzi l'emmagatzematge i / o tractament de dades personals.

- XIFRAT DE DADES: Quan es precisi realitzar l'extracció de dades personals fora del recinte on es realitza el seu tractament, ja sigui per mitjans físics o per mitjans electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació per garantir la confidencialitat de les dades personals en cas d'accés indegut a la informació.

- CÒPIA DE SEGURETAT: Periòdicament es realitzarà una còpia de seguretat en un segon suport diferent del que s'utilitza com a còpia primària. La còpia s'emmagatzemarà en lloc segur, diferent d'aquell en què estigui ubicat l'ordinador amb els fitxers originals, per tal de permetre la recuperació de les dades personals en cas de pèrdua de la informació.

GEDI estableix controls periòdics per assegurar que aquestes mesures tècniques de seguretat i d'altres estan implantades. (Veure punt 10 d'aquest document)

6.- GESTIÓ D'INCIDÈNCIES

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

El coneixement i la no notificació d'una incidència serà considerat com una falta contra la seguretat de les dades per part d'aquesta persona.

Qualsevol persona que tingui coneixement d'una incidència és responsable de comunicar-ho al **Responsable Seguretat Local (RSL)**, aquest a la vegada o farà al **Responsable Seguretat Global (RSG)** utilitzant el formulari FP002/F5 "Notificació i registre d'incidències".

Responsable Seguretat Global (RSG) serà responsable de realitzar l'anàlisi de les causes juntament amb les persones que consideri necessàries i establir les accions per a la seva resolució.

Un cop identificada, analitzada i establertes les accions per a la seva resolució es seguirà el procés descrit a FP001 Gestió de la qualitat i la millora del sistema de gestió de la qualitat.

S'agruparà en un arxiu el formulari FP002/F5 "Notificació i registre d'incidències" juntament amb totes les evidències. El temps de conservació d'aquest arxiu és d'un mínim de 5 anys.

6.1. NOTIFICACIÓ A L'AUTORITAT DE CONTROL D'UNA VIOLACIÓ DE LA SEGURETAT DE LES DADES PERSONALS

Quan es produeixin violacions de seguretat de dades de caràcter personal, com per exemple, el robatori o accés indegut a les dades personals, el Responsable Seguretat Global (RSG) ho notificarà a l'Agència Espanyola de Protecció de Dades en el termini de 72 hores, la notificació inclourà també tota la informació necessària per a l'aclariment dels fets que hagin donat lloc a l'accés indegut a les dades personals. En cas de no comunicar-se en el termini de 72 hores, la notificació ha d'anar acompanyada d'indicació dels motius de la dilació.

La notificació es realitzarà per mitjans electrònics a través de la seu electrònica de l'Agència Espanyola de Protecció de Dades a l'adreça: https://sedeagpd.gob.es

7.- PROCEDIMENTS DE CÒPIES DE SEGURETAT I RECUPERACIÓ

La seguretat de les dades personals comporta la integritat i la disponibilitat d'aquestes dades. Per a garantir aquests dos aspectes fonamentals, existeixin els procediments de còpies de seguretat i de recuperació de dades.

El **Responsable Seguretat Global (RSG)** serà responsable de definir la metodologia de realització de les còpies de seguretat i de les proves de recuperació. Aquests quedaran definits a l'Annex A "Recursos protegits" i a FP002/F7 "Recursos protegits per servei".

El **Responsable Seguretat Global (RSG)** serà responsable d'assignar la persona responsable de la realització de les còpies de seguretat i de les proves de recuperació. Les persones responsables es poden consultar al document "FP002/F7 Recursos protegits per servei".

7.1. CÒPIES DE SEGURETAT

El procés de còpia de seguretat ha de garantir la reconstrucció dels fitxers a l'estat que tenien en el moment de produir-se una eventual pèrdua o destrucció de les dades.

En el cas que calgui modificar o substituir hardware o traslladar les dades a un altre equip/base de dades/suport, abans de l'actuació s'ha de fer una còpia de seguretat de les dades.

7.2. PROVES DE RECUPERACIÓ

Com a mínim cada sis mesos s'ha de verificar que les còpies de seguretat s'estan fent correctament i es poden restaurar. Per fer-ho, ha d'aplicar els procediments sense afectar les dades reals.

Pels fitxers temporals resultants de les proves de recuperació s'ha de mantenir el mateix nivell de seguretat i un com finalitzada la verificació del procediment i si ja no són necessaris s'han d'eliminar de forma permanent.

Quan la restauració sigui conseqüència d'una incidència, si, entre la data en què es va fer la darrera còpia de seguretat i la data en què és necessari fer la restauració, la informació s'ha modificat i s'ha de recuperar manualment a partir de documentació en paper, aquesta circumstància s'ha de fer constar en el registre d'incidències amb el màxim detall possible.

Es registraran en el "FP002/F10 Restauració de còpies de seguretat" la verificació del procediment de recuperació així com totes les recuperacions extraordinàries.

8.- EXERCICI DE DRETS PELS INTERESSATS

8.1. TRANSPARÈNCIA DE LA INFORMACIÓ

GEDI SCCL prendrà les mesures oportunes per a facilitar a les persones interessades tota informació relativa al tractament de les seves dades de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill.

El formulari "FP002/F4 Llistat de clàusules informatives" recull la informació a facilitar a les persones interessades ja sigui per escrit o per altres mitjans.

8.2. EXERCICI DELS DRETS DE LES PERSONES INTERESSADES

Els drets de les persones interessades són:

Dret d'accés: Suposa el dret de l'interessat de dirigir-se a GEDI per conèixer si està tractant o no les seves dades de caràcter personal i, en el cas que s'estigui realitzant aquest tractament GEDI ha d'informar a l'interessat d'acord a l'article 15 del RGPD.

Dret de rectificació: L'exercici d'aquest dret suposa que la persona interessada obtingui de GEDI i sense dilació indeguda la rectificació de les seves dades personals inexactes. Tenint en compte les finalitats del tractament, té dret a que se li completin les dades que siguin incompletes mitjançant una declaració addicional. Aquest dret està regulat a l'article 16 del RGPD.

Dret d'oposició: Aquest dret suposa que la persona interessada es pot oposar a que GEDI realitzi un tractament de les seves dades personals en base a un interès legítim, incloent l'elaboració de perfils. En aquest cas GEDI deixarà de tractar les dades personals, llevat que acrediti motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions. Aquest dret està regulat a l'article 21 del RGPD.

Dret de limitació: La persona interessada té dret a obtenir de GEDI la limitació del tractament de les seves dades personal quan es compleixin alguna de les condicions contemplades a l'article 18 del RGPD.

Dret de portabilitat: Quan el tractament es faci per mitjans automatitzats en base al consentiment o en el marc de l'execució d'un contracte, la persona interessada té dret a que GEDI li faci arribar les dades en un format estructurat, d'ús comú, de lectura mecànica i interoperable, de forma que si ho desitja pugui transmetre'l a un altre responsable. Dins d'aquest dret també pot sol·licitar que GEDI transmeti les dades directament al nou responsable designat per la persona interessada. Aquest dret està regulat a l'article 20 del RGPD.

Dret de supressió: La persona interessada té dret a obtenir sense dilació indeguda de GEDI la supressió de les dades personals que li concerneixin tenint en compte l'article 17 del RGPD, així mateix la Llei Orgànica 3/2018 amplia la regulació respecte al "dret a l'oblit".

Dret a no ser objecte de decisions individuals automatitzades, inclòs l'elaboració de perfils: Tota persona interessada té dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat, inclou l'elaboració de perfils, que li produeixi efectes jurídics o li afecti significativament de manera similar. Aquest dret està regulat a l'article 22 del RGPD. GEDI no realitza aquesta tipologia de tractaments.

8.2.1. Drets i deures en l'exercici dels drets

- El seu exercici ha de ser gratuït.
- GEDI ha de respondre en el termini d'un mes. Es pot prorrogar dos mesos més, sempre que es pugui justificar la complexitat i/o nombre de sol·licituds.
- GEDI està obligada a informar sobre els mitjans per exercir aquests drets (sempre es facilitaran els models). No es pot denegar l'exercici dels drets si la persona interessada opta per altres mitjans.

- Si GEDI no dóna curs a la sol·licitud, informarà en el termini màxim d'un mes de les raons de la decisió i informarà de la possibilitat de reclamar davant de la Agencia Española de Protección de Datos.

8.2.2. Requisits de la sol·licitud per a ser tramitada

- La petició ha d'anar adreçada a GEDI i ha de concretar la petició de quin o quins drets vol exercir la persona interessada.
- S'ha d'acreditar la identitat de la persona interessada sol·licitant, com fotocòpia del NIF, passaport, document signat electrònicament o un altre document vàlid.
- Si s'exerceix a través d'un representant s'ha d'acreditar la representació.

8.2.3. Procediment

GEDI facilitarà els formats de la Agencia Española de Protección de Datos encara que la persona interessada pot utilitzar altres mitjans.

Quan qualsevol persona de GEDI rebi una sol·licitud d'exercici de drets ho comunicarà a **Responsable Seguretat Global (RSG).**

El **Responsable Seguretat Global (RSG)**:

- Revisarà la sol·licitud per comprovar que conté tota la informació i que la persona interessada adjunta document identificatiu. En cas d'estar incomplerta o inexacte, en el termini màxim d'un mes a comptar des de la recepció de la sol·licitud, es comunicarà a la persona interessada que completi la informació.
- Registrarà la sol·licitud al "FP002/F2 Registre exercici dels drets per part persones interessades", donarà les instruccions a les persones que correspongui
- Respondrà a la persona interessada en el termini màxim d'un mes a comptar des de la recepció de la sol·licitud.
- Verificarà i tancarà la sol·licitud.

9.- PRESTADORS DE SERVEIS. ENCARREGATS DEL TRACTAMENT

La realització de tractament per compte de tercers, encarregats del tractament, haurà d'estar regulada en un contracte per escrit o un altre document vàlid legalment que permeti acreditar la seva celebració i contingut. Veure models "FP002/F11 Clàusules proveïdors de serveis amb accés a dades" i "FP002/F12 Clàusules proveïdors de serveis sense accés a dades". En cas de no utilitzar aquests models es podrà utilitzar d'altres del propi proveïdor però hauran d'estar revisats pel **Responsable Seguretat Global (RSG)** per assegurar que contemplen tots els requisits del RGPD.

El **Responsable Seguretat Local (RSL)** portarà al dia el registre "FP002/F6 Llista de contractes de prestadors de serveis", on s'estableixen les diferents modalitats d'accés a les dades.

10.- RÈGIM DE TREBALL FORA DELS LOCALS

Totes les persones treballadores de GEDI tenen la possibilitat de realitzar el tractament de dades fora dels locals de GEDI (teletreball).

En l'Annex A "Recursos protegits" i a FP002/F7 "Recursos protegits per servei" es descriurà la forma d'accés i les mesures de seguretat establertes per garantir l'accés únicament a les persones autoritzades, que poden ser persones treballadores o prestadors de serveis.

Les persones que accedeixin remotament a les dades hauran d'aplicar les mateixes mesures de seguretat que si ho fessin de forma local, és a dir, complint amb les normes establertes a "FP002/F1 Clàusula informativa i compromís de confidencialitat" i que s'amplien a la normativa establerta al Manual de Seguretat.

Els prestadors de serveis que accedeixin remotament a les dades hauran de tenir signat un contracte com encarregats del tractament que els comprometi amb les mesures de seguretat establertes per la legislació vigent i per GEDI, aquest contracte es regirà pel previst en el punt 9 d'aquest Manual.

11.- CONTROLS PERIÒDICS DE LES MESURES DE SEGURETAT

GEDI ha establer dos mecanismes per la verificació, avaluació i valoració regular de l'eficàcia de les mesures tècniques i organitzatives establertes per garantir la seguretat del tractament de les dades de caràcter personal, així com que el tractament es realitza d'acord als requisits establerts en la legislació vigent en matèria de protecció de dades personals.

11.1. CONTROLS INTERNS DEL COMPLIMENT

GEDI estableix controls periòdics per assegurar que les mesures organitzatives i tècniques estan implantades, aquest controls es realitzaran a intervals planificats, mínim cada 6 mesos. Així mateix també es realitzaran quan es produeixin modificacions substancials a nivell organitzatiu i/o tècnic que puguin tenir repercussions en la seguretat de les dades.

El **Responsable Seguretat Global (RSG)** serà el responsable de que es realitzin aquests controls per part dels **Responsables Seguretat Local (RSL)** i que es registrin els resultats a "FP002/F13 Control del compliment" així com d'establir propostes de mesura correctores en cas d'identificar-se desviacions. El resultat d'aquest control serà presentats a l'Equip de Gerència per part del **Responsable Seguretat Global (RSG).**

Serà responsabilitat de l'Equip de Gerència dotar dels recursos necessaris per a la implantació de les mesures correctores.

12.- APROVACIÓ, REVISIÓ I DISTRIBUCIÓ D'AQUEST DOCUMENT

Aquest document haurà de mantenir-se permanentment actualitzat. Qualsevol modificació rellevant en els sistemes d'informació automatitzats o no, a l'organització dels mateixos, o en les disposicions vigents en matèria de seguretat de les dades de caràcter personal comportaran la revisió de la normativa inclosa i, si procedeix, la seva modificació total o parcial.

L'aprovació del Manual de Seguretat i de les seves posteriors modificacions correspon a **Responsable Seguretat Global (RSG).**

Les modificacions introduïdes en el Manual de Seguretat com a conseqüència de les revisions periòdiques, es detallaran en la Taula de revisions de la portada d'aquest document, indicant la data i els aspectes objecte de revisió.

Un cop revisat i aprovat el document s'actualitzarà a la carpeta de documentació vigent i es comunicarà a tot el personal tal com estableix la sistemàtica de distribució del sistema de gestió de la qualitat.

13.- ANNEX A. GESTIÓ DE RISCOS EN EL TRACTAMENT DE LES DADES

GEDI és una cooperativa de treball associat, sense ànim de lucre i d'iniciativa social.

Els tractaments realitzats per GEDI s'han recollit a FP002/F3 "Registre de Tractaments Activitats (RAT)".

A continuació es fa una anàlisi global de les dades tractades per establir si és necessari realitzar un anàlisi més detallat per algun dels tractaments.

L' activitat de GEDI es podria englobar en algun dels següents sectors?

	Sanitari
x	Activitats de serveis socials

GEDI tracta alguna de les següents categories especials de dades?

x	Dades de salut física o mental
x	Dades relatives a la vida sexual o a l'orientació sexual

GEDI realitza algun dels següents tractaments amb les dades?

	Fa o analitza perfils
	Fa publicitat i prospecció comercial massiva a potencials clients
	Presta serveis d'explotació de xarxes públiques o serveis de comunicació electrònica (proveïdor de serveis d'Internet segons Llei General de Telecomunicacions)
	Gestiona els associats o membres de partits polítics, sindicats, esglésies, confessions o comunitats religioses, fundacions i altres entitats sense ànim de lucre, la finalitat de les quals sigui política, filosòfica, religiosa o sindical.
	Gestió, control sanitari o venda de medicaments
	Historial clínic o sanitari

GEDI realitza transferència de dades a tercers països?

	Països de la UE
	Països fora de la UE amb reconeixement de nivell de protecció adequada segons el Diari Oficial de la Unió Europea.
	Països fora de la UE sense reconeixement de nivell de protecció adequada
x	Cap de les anteriors

Segons les respostes anteriors, GEDI realitza tractament de dades especialment sensibles que suposen un risc per als drets i llibertats dels interessats **"TRACTAMENT EXPEDIENTS PERSONES USUÀRIES"** per aquest tractament s'ha realitzat una avaluació segons **FP002/F8 Informe "Evaluación impacto"**.

Tots els tractaments recollits a "FP002/F3 Registre Activitats de Tractament (RAT)" es sotmeten a un anàlisi de riscos d'acord a la sistemàtica definida al sistema de gestió de la qualitat FP103 "Gestió dels riscos".

L'anàlisi queda recollida i registrada a **"FP103/F1 Avaluació de riscos LOPDGDD".** Aquesta anàlisi es revisarà:

- De forma periòdica, com a mínim un cop a l'any.
- Quan hi hagin canvis en les dades gestionades.
- Quan hi hagin canvis en els serveis prestats.
- Quan es registrin incidències greus de seguretat o es reportin vulnerabilitats del sistema.

14.- ANNEX B. FUNCIONS I OBLIGACIONS

14.1. RESPONSABLE DE SEGURETAT GLOBAL (RSG)

- Gestionar el sistema de seguretat de les dades de caràcter personal durant tot el seu cicle de vida.
- Realitzar l'anàlisi i gestió de riscos del sistema.
- Determinaran les mesures tècniques i organitzatives apropiades per garantir i acreditar que el tractament es realitza de conformitat amb el RGPD, la LOPGDD i normes de desenvolupament.
- Aprovar el FP002/F3 Registre d'activitats de tractament (RAT).
- Elaborar i implantar la normativa de seguretat creant un document (Manual de seguretat) d'obligat compliment pel personal amb accés a les dades de caràcter personal i als sistemes d'informació. També tindrà l'obligació de mantenir-lo actualitzat en tot moment i adequat a les disposicions legalment vigents en cada moment.
- Establir les funcions i obligacions del personal així com el personal assignat a cada funció. Així mateix, haurà d'adoptar les mesures necessàries perquè el personal conegui les normes de seguretat que afecten al desenvolupament de les seves funcions i les conseqüències en cas d'incompliment de les mateixes.
- Analitzar els informes dels controls periòdics i de les auditories, així com elevar-ne les conclusions a l'Equip de Gerència.
- Gestió i seguiment d'incidències.
- Serà el màxim responsable en les comunicacions amb l'Agencia Española de Protección de Datos.

14.2. RESPONSABLE DE SEGURETAT LOCAL (RGL)

- Conèixer la normativa de seguretat interna de l'organització.
- Coordinar i controlar les mesures establertes en el Manual de Seguretat a nivell de la seva àrea.
- Serà la interfase en matèria de seguretat amb el **Responsable Seguretat Global (RSG)**.
- Realitzar amb la periodicitat establerta el Control de periòdics del sistema a la seva àrea i traslladar els resultats al Responsable de Seguretat Global.
- Comunicar a tot el personal de la seva àrea les obligacions en relació a la protecció de les dades de caràcter personal.
- Comunicar al **Responsable de Seguretat Global (RSG)** les incidències que es produeixin a la seva àrea.

14.2. ADMINISTRADORS DEL SISTEMA I DE LES APLICACIONS

- Gestionar els permisos d'accessos a les dades a través de sistemes informatitzats.
- Informar al **Responsable Seguretat Global (RSG)** de les altes i baixes dels usuaris a les aplicacions.
- Conèixer la normativa interna en matèria de seguretat, i especialment la referent a la gestió d'usuaris.
- Utilitzar els controls i mesures que s'hagin establert per protegir tant les dades de caràcter personal com els propis sistemes d'informació i els seus components: els fitxers automatitzats, els programes i els suports i els equips utilitzats per l'emmagatzemament i tractament de les dades de caràcter personal.

14.3. USUARIS

- Conèixer la normativa de seguretat interna de l'organització.
- Aplicar les mesures tècniques i organitzatives establertes en el Manual de Seguretat en el seu àmbit de treball.
- Comunicar al **Responsable Seguretat Local (RSL)** les incidències que es produeixin en matèria de protecció de dades.

15.- ANNEX C. DEFINICIONS

«DPC» Dades caràcter personal

«RAT» Registre d'activitats de tractaments (FP002/F3)

«AEPD» Agencia Española de Protección de Datos

«RGPD» Reglament General de Protecció de Dades (Reglament (UE) 2016/679, de 27 d'abril de 2016)

«LOPDGDD» Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (Llei Orgànica 3/2018, de 5 de desembre)

«dades personals» (art. 4 RGPD) : tota informació sobre una persona física identificada o identificable («l'interessat»); es considerarà persona física identificable tota persona la identitat pugui determinar, directament o indirectament, en particular mitjançant un identificador, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona;

«tractament» (art. 4 RGPD): qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, confrontació o interconnexió, limitació, supressió o destrucció;

«responsable del tractament» (art. 4 RGPD): la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determini els fins i mitjans del tractament; si el Dret de la Unió o dels Estats membres determina els fins i mitjans del tractament, el responsable del tractament o els criteris específics per al seu nomenament podrà establir-los el Dret de la Unió o dels estats membres;

«encarregat del tractament» (art. 4 RGPD): la persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament;

«consentiment de l'interessat» (art. 4 RGPD): tota manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, ja sigui mitjançant una declaració o una clara acció afirmativa, el tractament de dades personals que el concerneixen;

«violació de la seguretat de les dades personals» (art. 4 RGPD): tota violació de la seguretat que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o accés no autoritzat a aquests dades;

«Avaluació d'impacte en la protecció de dades personals» és l'anàlisi dels riscos que un determinat sistema d'informació, producte o servei pugui implicar per a les dades de caràcter personal tractades per l'organització.

16.- DOCUMENTACIÓ COMPLEMENTÀRIA

FP001 Gestió integral qualitat i millora contínua
FP103 Gestió dels riscos i les oportunitats