Des de 1961
aspace
Associació de la Paràlisi Cerebral
DECLARADA D'UTILITAT PÚBLICA
Ordre 23/02/1968
Ministerio del Interior

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

V1.0.5 - FEBRER 2017

Control de versions

Data i Versió	Persona	Descripció
17/03/2015 – 1.0	Paul Mussach/ Yolanda Elipe	Primera versió del document de Política de Seguretat de la Informació.
06/11/2015 - 1.0.1	Paul Mussach	Revisió: identificació d'usuaris i proves semestrals de recuperació d'informació.
02/03/2016 – 1.0.2	Paul Mussach	Afegim l'annex 17 de procediment de registre d'accessos.
06/04/2016 – 1.0.3	Paul Mussach	Afegim l'annex 18 de política de desenvolupament.
25/01/2017 – 1.0.4	Paul Mussach	Afegim l'annex 19 de pautes d'ús dels mòbils.
08/02/2017 – 1.0.5	Paul Mussach	Afegim l'annex 20 de procediments d'arxiu físic
15/03/2017 – 1.0.6	Paul Mussach	Afegim els annexes 21 i 22

Signatures

Elaborat per: Yolanda Elipe i Paul Mussach	Revisat per: Carles Sanrama	Aprovat per: Carles Sanrama
Data: 17/03/2015	Data: 17/03/2015	Data: 17/03/2015

Des de 1961

aspace

Associació de la Paràlisi Cerebral

DECLARADA D'UTILITAT PÚBLICA
Ordre 23/02/1968
Ministerio del Interior

CIF - G-08393936. Domicili fiscal: C/ Tres Pins, 31-35 (Parc de Montjuïc). 08038, Barcelona

Associació de la Paràlisi Cerebral

C/ Tres Pins, 31-35 (Parc de Montjuïc) / 08038 Barcelona
Telf: 93 325 83 00 / Fax: 93 325 83 62 / aspace@aspace.cat

Índex

1 Objecte

L'objectiu principal d'aquest document és establir les mesures, normes i procediments que afecten als fitxers automatitzats i no automatitzats, així com als llocs de treball, equips, sistemes i programes que intervenen en el tractament de les dades de l'**Associació de Paràlisi Cerebral**, per tal de garantir la seva confidencialitat, disponibilitat, fiabilitat i integritat i fer-ho d'acord a la normativa de referència.

A la vegada, es pretén aconseguir un ús racional i optimitzat dels recursos informàtics existents a ASPACE tot acomplint les normes legals vigents.

Un cop aprovada, aquesta política serà d'obligat compliment per a tota l'organització. No obstant, caldrà:

- Reflectir tots aquells punts que afectin el personal d'Aspace a la normativa interna i comunicar-la.
- Adaptar i implementar els diferents processos (informàtics i de negoci) per a plasmar els requeriments que figuren a aquesta política.

2 Referències legals

La llei 15/1999 de 13 de desembre de protecció de dades de caràcter personal, així com el reial decret 1720/2007 de 21 de desembre, que n'aprova el reglament de desenvolupament.

Aquestes normatives obliguen a mantenir la confidencialitat de les dades de caràcter personal enregistrades durant i per la realització de la nostra activitat quotidiana. La nostra institució compta en l'actualitat amb sis fitxers declarats a l'AEPD: comunicació i socis, recursos humans, administració, pacients, videovigilància i investigació clínica. A l'Annex 0 se'n detallen les principals característiques de cada un d'ells.

3 Àmbit d'aplicació:

- **Tipus d'informació:**

  - Segons la LOPD, s'entén per **dades de caràcter personal**:

    "Qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que fa referència a persones físiques identificades o identificables."

    Per tant, són dades de caràcter personal nom, cognoms, data de naixement, adreça postal, adreça de correu electrònic, número de telèfon, NIF, empremta digital, l'ADN, una fotografia, un vídeo, la gravació de la veu, número de seguretat social, etc.

  - També segons la LOPD s'entén per **fitxer**:

    "Tot conjunt organitzat de dades de caràcter personal, que permeti l'accés a les dades d'acord a criteris determinats, qualsevol que sigui la forma de creació, emmagatzemament, organització i accés".

    S'inclouen tant els fitxers automatitzats (informatitzats) com els no automatitzats. Però han de ser organitzats i estructurats per a permetre l'accés a les dades de les persones.

- **Ubicacions:**

  - La present política s'aplicarà a tot l'àmbit territorial d'actuació d'Aspace, i per tant inclou tots els seus centres de treball i personal, així com les activitats fora dels centres organitzades per Aspace. Els procediments concrets d'aplicació per a cada centre i activitat s'adaptaran a les seves particularitats i possibilitats tècniques.

- **Abast:**

  - La present política tindrà en compte tots els serveis i departaments dins d'Aspace que tinguin relació amb la informació de caràcter personal. Per tant, inclourà tots aquells aspectes relacionats amb les tecnologies de la informació, però també aspectes administratius i d'organització.

- **Fitxers:**

  - Aquesta política afecta a tota la informació de caràcter personal d'Aspace. Per tant, inclou tots els fitxers declarats a l'AEPD actualment i els que es puguin declarar en el futur, sigui quin sigui el seu nivell de seguretat d'acord amb la LOPD.

  - No obstant l'anterior, la manera com es protegeix la informació i els procediments específics sí que podran ser diferents per a cada fitxer atenent al seu nivell de seguretat.

- **Persones jurídiques:**

  - La política comprèn les següents figures jurídiques:

    a. Associació de la Paràlisi Cerebral – G08393936
    b. Institut Aspace Fundació privada – G63095376
    c. Les empreses externes que tracten o tenen accés a les dades d'Aspace (a les quals vincularà a través de clàusules en els contractes de servei).
    d. Totes les figures vinculades a Aspace que es puguin crear en el futur.

4 Polítiques de seguretat de la informació

4.1 Captació

Per tal de poder incorporar dades de caràcter personal als fitxers propietat d'Aspace cal informar la persona (o el seu tutor legal, si és el cas) de la incorporació, la finalitat del fitxer i dels seus drets ARCO i tenir el seu consentiment explícit o implícit.

Qualsevol informació de caràcter personal que arribi i que no s'hagi d'incorporar als fitxers (o per la que no es disposi d'autorització) s'haurà de destruir de forma immediata.

4.1.1 Autorització (prèvia o puntual)

Totes les persones de les quals incorporem dades als fitxers d'Aspace han d'autoritzar aquesta incorporació. Aquestes autoritzacions inclouran de forma genèrica les finalitats i els tractaments més comuns que se li dóna a la informació, així com el nom del fitxer a on s'inclouran les dades. Veure l'Annex 4 amb els diferents models d'autoritzacions. Això afecta a:

- Personal professional d'Aspace
- Personal voluntari d'Aspace (eventual o no)
- Pacients i usuaris dels serveis d'Aspace (i els seus familiars)
- Socis d'Aspace i patrons de la Fundació
- Proveïdors d'Aspace
- Destinataris de les comunicacions d'Aspace

En el cas d'activitats que per la seva rellevància o eventualitat quedin fora de l'autorització inicial, cal fer una autorització específica.

També caldrà demanar una nova autorització en el cas que canviïn les finalitats dels fitxers o els usos que se'n fan.

4.1.2 Incorporació al fitxer

Existeixen diversos mitjans per a captar les dades de caràcter personal. Cada un d'ells tindrà les seves especificitats, però sempre cal assegurar que la informació sigui tractada d'acord amb la present política.

- Dades en paper
- Dades via web (formularis)
- Dades via telemàtica
- Informació generada internament

4.1.3 Captació de CVs

Existirà una porta d'entrada de CVs comuna per tot Aspace, que estarà ubicada a la web corporativa:

- El formulari **"Treballa amb nosaltres"** (http://aspace.cat/ca/colabora/treballa-amb-nosaltres) per als professionals. Readreça al correu rrhhcv@aspace.cat.
- El formulari **"Fes-te voluntari"** (http://aspace.cat/ca/colabora/fes-te-voluntari) per als voluntaris. Readreça al correu voluntariatcv@aspace.cat.

Ambdós formularis (i els que es puguin crear més endavant) inclouran els avisos legals pertinents, i en cas de demanar que els CVs s'enviïn a una adreça de correu, aquesta adreça inclourà una resposta automàtica amb el mateix avís legal.

No s'acceptaran CVs en paper (es rebutjaran o seran destruïts de forma immediata i segura), ni en qualsevol altre mitjà (fax, e-mail, etc), i s'indicarà als interessats/des que s'adrecin a la web.

4.2 Emmagatzemament i transport

Aspace ha de garantir la seguretat i la correcta conservació de la informació. Per tal d'assolir-ho de forma òptima cal minimitzar les duplicitats i els llocs físics a on aquesta informació està emmagatzemada.

4.2.1 Repositoris de la informació

Aspace emmagatzema la informació corporativa tant en suport informàtic com en paper. A continuació es descriuen els aspectes més rellevants en matèria de seguretat relatives a aquests repositoris.

Repositoris físics (paper)

Aspace té una estratègia encaminada a la digitalització de tota la seva documentació i arxius de treball. No obstant, encara disposa d'una gran quantitat d'arxius físics en format paper, distribuïts pels diversos centres, que contenen informació de tots els nivells de seguretat.

En particular, la Història Clínica de tots els pacients atesos per Aspace (arxiu actiu d'adults i arxiu actiu de pediatria) està ubicada a l'Arxiu Central del Centre Pilot (c/ Tres Pins 31-35).

El llistat complert de tots els repositoris físics en format paper està al Registre 1a d'arxius físics d'informació (especificat en l'Annex 1 - Registres).

Aquest registre inclou informació sobre:

- Ubicació de l'arxiu
- Tipus d'informació que conté i finalitat
- Criteri d'arxiu (ordenació, etc.)
- Qui hi té accés
- Mesures de seguretat

Aquest document s'actualitzarà anualment per tal de recollir els canvis que s'hagin produït.

Al marge dels repositoris presents als centres d'Aspace, l'entitat té contractat un servei extern de custòdia i gestió integral de la informació amb MBA Archivos. Allà s'hi emmagatzema i es tracta la informació clínica que actualment no està en ús.

Repositoris informàtics

Aspace manté un grup de servidors institucionals principals, ubicats en:

- Sala de servidors (CPD) del Centre Pilot (c/ Tres Pins 31-35)
- Sala de servidors (CPD) del Centre Integral Montjuic (c/ Tres Pins 29)

Aquests servidors constitueixen els repositoris principals de totes les dades de caràcter personal, en particular d'aquelles que estan automatitzades.

De la mateixa manera, cada centre té el seu propi servidor satèl·lit per tal de facilitar la disponibilitat de la informació més immediata que els centres necessiten per al seu treball del dia a dia. La informació existent en aquests servidors es replica de manera continuada en els servidors institucionals principals.

En alguns casos la informació pot residir en servidors externs a Aspace (model de serveis en el núvol). En aquests casos el servei ha de complir tots els requeriments legals de la Llei de Protecció de Dades i en particular cal disposar del contracte d'encarregat de tractament corresponent.

Addicionalment, Aspace disposa d'equips i suports de contingència i còpia de seguretat a on es conserven versions antigues de tota la informació. Aquests suports poden traslladar-se fora de les dependències d'Aspace (per exemple a una caixa de seguretat d'un banc) en funció del que es concreti d'acord amb la política de còpies de seguretat.

Tots els servidors i altres dispositius amb informació de caràcter personal han d'estar etiquetats i han de ser inclosos al Registre de Repositoris (1b per a servidors i 1c per a altres dispositius), fent-hi constar com a mínim:

- Nom de l'equip o dispositiu (que ha de coincidir amb l'etiqueta identificativa). Aquest nom ha de seguir l'estàndard definit a l'Annex 6 - Política d'identificació d'equips.

- Data d'alta o entrada en funcionament del dispositiu
- Sistema operatiu/sistema d'arxius
- Ubicació física
- Tipus d'informació que conté
- Fitxers (declarats a l'AEPD) als que pertany la informació
- Persones autoritzades a accedir-hi físicament
- Persones autoritzades a accedir-hi lògicament (usuaris administradors de la màquina)

No s'ha d'emmagatzemar cap informació rellevant en els equips de treball, sempre s'ha de treballar directament amb la informació al servidor corresponent accedint via la xarxa informàtica. En la mesura que tècnicament sigui viable, això implicarà la configuració de:

- Perfils mòbils
- Redirecció de carpetes
- Accés via escriptoris virtuals
- Bloqueig de l'accés als discos locals

Excepcionalment es pot emmagatzemar informació en local en els equips de treball de forma temporal, amb una raó justificada i amb autorització per part del responsable del centre. Un cop la raó desapareix la informació cal traspassar-la de nou al servidor, assegurant-se que no es perdin modificacions que es puguin haver fet al servidor i que a l'equip local no quedi cap rastre de la informació.

Mai s'ha d'extreure aquesta informació fora de les instal·lacions d'Aspace si no és per les causes previstes en els punts següents.

Repositoris externs a Aspace

Arxiu físic per a la custòdia de documents: MDA Archivos.

Servidors externs que emmagatzemen algun tipus d'informació propietat d'Aspace, per accessos de tipus cloud. Actualment i en un futur proper:

- Iwith (Suïssa). Properament deixarem de fer-ho servir.
- Google (Google Drive RRHH, informàtica...)
- Cezanne (Irlanda)
- Microsoft (Office 365)
- Digital Ocean (hosting web - Amsterdam)

Aquests repositoris externs han d'estar identificats com a encarregats de tractament i cal verificar que compleixin amb els requeriments legals corresponents.

4.2.2 Política d'arxiu de documents físics

Qualsevol dels arxius físics d'Aspace hauran de complir les mesures previstes per la llei de protecció de dades. En particular això inclou:

- **Criteris d'arxiu**: La documentació s'arxiva sota criteris que garanteixen la correcta conservació dels documents, localització, consulta i possibilitat d'exercici de Drets ARCO.

- **Restriccions d'accés** a les persones no autoritzades: Els arxius es troben en tot moment tancats amb clau.

- **Custòdia dels suports**: Quan la documentació no es trobi arxivada en els dispositius d'emmagatzemament, per estar en procés de revisió o tramitació, sigui prèvia o posterior al seu arxiu, el treballador que es trobi al càrrec de la mateixa haurà de custodiar-la i evitar en tot moment els accessos de terceres persones no autoritzades. Una vegada finalitza la seva utilització es procedirà al seu arxiu.

- **Destrucció segura** de la informació.

- **Còpia o reproducció**: la generació de còpies o la reproducció dels documents únicament podrà ser realitzada sota el control del personal autoritzat. S'haurà de procedir a la destrucció de les còpies o reproduccions rebutjades per tal d'evitar l'accés a la informació o la seva recuperació posterior.

En l'annex 20, de procediment d'arxiu físic es descriu en detall els processos a seguir per a la creació, manteniment i el·liminació de qualsevol arxiu físic a Aspace.

Qualsevol trasllat o moviment de documents físics amb dades de caràcter personal que impliqui la seva sortida de les dependències d'Aspace haurà d'estar expressament autoritzada pel responsable del fitxer, a més de complir amb els requeriments descrits en l'apartat de transport físic de suports.

4.2.3 Característiques dels servidors

Els equips informàtics que han d'actuar com a repositoris de la informació corporativa han de complir amb uns requeriments físics que permetin garantir al màxim la disponibilitat de la informació, així com les prestacions requerides.

Aquests requeriments són els següents:

- Redundància d'emmagatzemament:
    a. Servidors windows (aplicacions, domini, etc.): RAID 1

b. Servidors NAS (backup): RAID 5
- Font d'alimentació redundant
- Connexió de xarxa redundant

4.2.4 Política de suports informàtics

Com a norma general la informació propietat d'Aspace no s'ha d'emmagatzemar en cap suport fora dels servidors i eines de còpia de seguretat previstos. En particular no s'ha de fer servir cap mena de suport informàtic (discos externs, DVDs, pen-drives, telèfons mòbils, targetes de memòria, etc.) per a emmagatzemar informació ni per a fer còpies de la informació, degut als problemes de seguretat (facilitat de trasllat, possibilitat de pèrdua i/o sostracció, etc.) que això pot implicar.

Són excepcions a aquesta norma les següents:

- Còpies de seguretat de la informació (planificades i realitzades pel departament de Sistemes).
- Entrega d'informes i/o documentació a pacients i usuaris. S'entregaran en format paper o en un format digital (pdf) que no admeti modificacions. Només es podrà entregar informació personal a l'interessat o al seu tutor legal.
- Equips portàtils o suports assignats a persones amb tasques que requereixin mobilitat entre centres o fora d'Aspace, quan requereixin transportar informació per la impossibilitat (o poca operativitat) d'accedir a aquesta des del punt alternatiu de treball.
- Requeriment administratiu o judicial d'informació.
- Sol·licitud raonada i degudament autoritzada pels responsables de fitxer implicats.

En aquells casos que s'acceptin, els suports sempre han de ser propietat d'Aspace, i s'han d'etiquetar, encriptar (si s'escau) i protegir per contrasenya per tal de minimitzar-ne el risc d'accessos indeguts en cas de pèrdua o sostracció. Tant l'encriptació com la contrasenya compliran amb la política que es defineix en els punts posteriors, i seran efectuats pel departament d'informàtica.

4.2.5 Política BYOD (Bring Your Own Device)

Els sistemes d'Aspace estan preparats per a treballar amb els dispositius propietat d'Aspace, que hauran estat convenientment configurats pel departament TIC d'acord amb els paràmetres establerts a la present política.

No obstant això, es permetrà de forma limitada l'accés als recursos informàtics d'Aspace amb dispositius personals i/o l'ús dels mateixos en l'entorn de treball en els casos següents:

- **WIFI pública per accés a internet,** sempre que no suposi un risc de saturació de la xarxa de comunicacions.
- **Ús de portàtils i tablets personals amb finalitats educatives.** Especialment en el cas d'equips pertanyents als usuaris o als professionals dels serveis de l'escola o dels CTOs.
- **Ús de mòbils personals per a fer fotos o enregistrar vídeos d'usuaris,** sempre de forma excepcional i d'acord amb el que s'estableix a l'annex 19, de pautes d'ús de mòbils personals.

En general no es permetrà l'ús d'ordinadors portàtils personals en l'entorn de xarxa d'Aspace, si bé en ocasions se'n podrà habilitar l'ús temporal en cas de necessitat urgent. També se'n podrà habilitar un accés via VPN a la xarxa d'Aspace, però en tot cas això ho farà el departament TIC després d'haver verificat que l'equip compleix els requeriments de seguretat necessaris.

No es permet l'ús de càmeres digitals o altres dispositius d'enregistrament d'imatges que no siguin propietat d'Aspace. Tampoc no es permet l'ús de pen-drives o altres dispositius d'emmagatzemament massiu d'informació que no siguin propietat d'Aspace.

4.2.6 Transport físic de suports

En cas que calgui transportar suports amb informació, cal prendre precaucions per tal d'evitar que la seva pèrdua o sostracció pugui propiciar accessos indeguts.

Com a consideració inicial, sempre que sigui possible, cal optar per enviar la informació de forma telemàtica, d'acord amb el punt que s'explica posteriorment. Això redueix la duplicació de la informació i n'elimina punts de vulnerabilitat.

Documents en paper o suports no susceptibles d'encriptació

El transport ha de ser segur i per a això hi ha dues opcions:

- Mitjançant empresa de missatgeria o transport que garanteixi la confidencialitat i seguretat de la informació.
- En cas de ser transportat per mitjans propis, cal fer servir sobres o altres contenidors tancats. En el cas que la informació sigui de nivell alt caldrà utilitzar un maletí o caixa de seguretat tancat amb clau.

Suports encriptables (discos durs, USBs, targetes de memòria, etc.)

S'ha de procedir a l'encriptació com a forma prèvia a la sortida del transport.

Dispositius portàtils (ordinadors portàtils, tablets, smartphones, etc.)

Cal assegurar que tota la informació estigui encriptada. Això s'implementarà de la forma següent:

- Encriptant el dispositiu sencer (quan sigui tècnicament viable)
- Encriptant una part del dispositiu. Caldrà en aquest cas que la informació resideixi en la part encriptada.
- Si no és possible fer cap sistema d'encriptació a nivell de dispositiu, caldrà emmagatzemar la informació encriptada per altres mitjans que determini el departament TIC.

Consideracions addicionals

A banda de l'anterior, cal:

- Etiquetar i registrar el suport.
- Anotar qualsevol entrada o sortida de suports informàtics o en paper en el Registre 3 d'entrades i sortides, d'acord amb el procediment descrit a l'Annex 17.

En cas d'haver de traslladar físicament servidors, discos o altres dispositius que puguin portar informació, cal complir també amb els requeriments abans descrits. L'única excepció acceptable és en el cas d'una situació de contingència, quan el compliment d'aquesta política impliqui un retard important en la recuperació del servei.

El cas concret dels suports, dispositius i dades que es necessiten per a les sortides del servei de lleure i respir es descriu a l'Annex 21, de procediment per a sortides de lleure i respir.

4.2.7 Enviament telemàtic d'informació

Les dades que corresponen a nivell alt de seguretat (particularment les dades de salut) que s'envien per mitjans telemàtics (correu electrònic o diferents eines al núvol) cal protegir-les per mitjà de sistemes d'encriptació punt a punt, de forma que cap proveïdor de serveis intermig hi tingui accés.

Les dades de caràcter personal de nivell baix o mig no es veuen afectades per aquesta política.

En funció del canal, les restriccions poden variar:

Transferència interna d'informació via carpetes compartides

És la forma més segura d'enviament intern d'informació, però caldrà evitar deixar informació de nivell alt (ni que sigui de forma temporal) en carpetes a on puguin tenir accés personal no autoritzat a accedir a la informació que es comparteix. En cas contrari, caldrà xifrar la informació d'acord amb el procediment descrit a l'Annex 2 – Procediment d'encriptació segura d'arxius.

Fax

No es pot fer servir per a enviar dades de nivell alt, donat que és un mitjà intrínsecament insegur que no permet el xifratge de la informació. Sí que es pot fer servir, prèvia verificació per part dels responsables de seguretat, si les dades estan correctament dissociades.

Correu electrònic

El correu electrònic, encara que els destinataris siguin interns d'Aspace, viatja per Internet de forma insegura per defecte. Quan s'hagi d'enviar informació sensible caldrà seguir el procediment d'encriptació segura d'arxius (especificat a l'Annex 2), demanar confirmació de recepció i posteriorment esborrar el correu (per tal d'evitar que en quedi còpia al servidor de correu electrònic).

D'altra banda, s'ha d'assegurar que la comunicació amb el servidor de correu d'Aspace sigui xifrada:

- En cas d'utilitzar eines client (ex. Outlook) caldrà fer servir protocols segurs (SSL o TLS) i els ports corresponents, en funció del servidor de correu utilitzat.
- En cas d'utilitzar webmail, la connexió haurà de ser segura (HTTPS).

Eines d'enviament de fitxers (WeTransfer, YouSendIt, etc.)

Per a volums molt grans (>10 MB) es fan servir aplicacions web especialitzades. En el cas que la informació a enviar sigui sensible cal assegurar-se que l'aplicació que es faci servir compleixi amb les garanties de seguretat, i en particular: seguretat d'accés (permisos i contrasenyes), custòdia i destrucció de la informació. De nou caldrà seguir d'encriptació segura d'arxius (especificat a l'Annex 2).

Eines de sincronització i còpia de seguretat (Dropbox, Google Drive, SkyDrive, etc.)

Malgrat la seva utilitat, no es permet al personal d'Aspace l'ús d'aquest tipus d'eines per a emmagatzemar dades de caràcter personal de qualsevol dels fitxers propietat d'Aspace.

Eines de control i accés remot (TeamViewer, VNC, LogMeIn, etc.)

No es permet al personal d'Aspace l'ús d'aquest tipus d'eines per a connectar-se des de fora de les instal·lacions d'Aspace. Les excepcions a aquesta norma es recullen en l'apartat de seguretat perimetral.

Altres eines

Per a l'ús d'altres eines no identificades en la política, caldrà requerir la validació per part del departament de sistemes i la posterior autorització per part dels responsables dels fitxers implicats.

4.3 Custòdia i destrucció

La política de seguretat ha de garantir que la informació emmagatzemada es conserva de forma segura durant tota la seva vida útil i durant el temps addicional que s'estableixi legalment en funció del tipus d'informació (exemple: els logs del registre d'accessos són dos anys; la informació comptable són 5 anys; etc.). Aquests temps addicionals es recullen en l'Annex 7 - Obsolescència de la informació.

També ha de garantir que un cop passi aquest temps, o quan es requereixi per altres situacions, es procedeixi a la destrucció segura de la informació, de forma que aquesta no es pugui recuperar.

Els següents apartats descriuen les polítiques concretes per a assolir aquests objectius.

4.3.1 Seguretat física

Les ubicacions físiques a on estan els arxius físics, servidors i altres dispositius d'emmagatzemament han de complir els següents requisits de seguretat:

- Estar sempre tancades amb clau.
    a. Les claus hauran d'estar guardades i en possessió (o a l'abast) només de les persones autoritzades.
- Accés restringit.
    a. Les persones autoritzades a accedir-hi seran els que constin en el Registre 1 de repositoris.
    b. Com a norma general no es permetrà l'accés a persones no autoritzades, tant de dins com de fora d'Aspace. En el cas d'autoritzar-se algun accés puntual, s'haurà d'anotar en el Registre 2 d'accessos físics, indicant dia, hores d'entrada i sortida, dades de la persona que entra i dades de la persona que autoritza.
- Seguretat anti-incendis.
    a. Les ubicacions han de tenir un sistema anti-incendis propi o com a mínim extintors compatibles amb sistemes electrònics en el cas dels servidors (els millors són els de CO2).
    b. El personal responsable de la coordinació en cas d'incendi en cada centre ha d'estar format, conèixer els protocols d'actuació i tenir present quins repositoris d'informació existeixen i on estan ubicats.
- Refrigeració de servidors

a. Les ubicacions de servidors han d'estar refrigerades i la temperatura monitoritzada. La temperatura ha de ser programada entre 18ºC i 22ºC.
b. La refrigeració no s'ha de situar en la vertical dels servidors, i ha de tenir mecanismes anticondensació que evitin goteigs en cas de fuites.

- Sistemes d'alimentació ininterrompuda (SAI)
    a. Els servidors i dispositius amb informació hauran d'estar protegits davant de caigudes de l'alimentació mitjançant SAI.
    b. En cas de detectar una falla d'alimentació el SAI haurà de sostenir l'alimentació dels dispositius connectats almenys durant 15 minuts, de forma que puguin ser apagats de forma controlada.
    c. Addicionalment, en cas de falla haurà de
        i. Emetre un avís sonor que sigui perceptible des dels despatxos i estances properes.
        ii. Enviar un avís via telemàtica (correu electrònic, SMS, etc.) als administradors de sistemes.
    d. En cas de caiguda d'alimentació fora de l'horari de treball, caldrà establir un sistema que aturi de forma controlada i automatitzada els servidors.
    e. Òptimament, les ubicacions haurien de tenir una doble escomesa d'alimentació, procedent de centrals diferents, i connectades a fonts d'alimentació redundants en cada servidor.
    f. Els CPDs més crítics (a on s'ubiquin els servidors centrals d'Aspace) hauran de quedar protegits per grups electrògens, que s'activaran automàticament en cas que es detecti una caiguda d'alimentació.

4.3.2 Seguretat perimetral

Seguretat física

Tots els centres d'Aspace a on hi hagi dades de caràcter personal han de disposar d'un sistema d'alarma connectat a una central d'alarmes que permeti detectar intrusions fora dels horaris de treball.

Seguretat lògica

Com a norma general no es permeten els accessos telemàtics des de l'exterior als sistemes d'Aspace. Com a mesures de seguretat per tal d'acomplir aquesta missió, hi ha:

- La configuració de firewalls per tal de restringir o bloquejar els intents d'accés des de l'exterior.
- El registre i la monitorització dels intents d'accés.

Una excepció són les aplicacions que resideixen dins dels sistemes d'Aspace però que han de ser accessibles des d'Internet. Per a aquests casos existeix una zona desmilitaritzada (DMZ) de forma que els accessos a les aplicacions no impliquin risc per a la seguretat de la resta de la xarxa.

Un altre cas són les aplicacions d'Aspace hostatjades en servidors externs (cloud), com per exemple la web, l'aplicació de RRHH i les que s'estableixin. En aquest cas la seguretat la proporcionarà el proveïdor de serveis, però en tot cas haurà de ser coherent amb la present política.

Les aplicacions accessibles des de l'exterior quedaran registrades en el Llistat d'Aplicacions Accessibles des de l'exterior (Registre 8), a on figurarà la ruta d'accés (URL, IP i port), el servidor físic (o virtual) a on resideix l'aplicació i els usuaris o criteris d'accés.

Accessos remots

En determinats casos, i amb l'autorització de la direcció es pot permetre l'accés remot per alguna de les causes següents:

- Teletreball
- Manteniment de sistemes i de servidors
- Manteniment d'aplicacions
- Accés a aplicacions

El departament de Sistemes és el responsable d'habilitar, mantenir, restringir i desactivar aquests accessos. Com a norma general estan limitats en el temps i s'han d'inscriure en el **Llistat d'autoritzacions per a accés remot** (Registre 7, descrit a l'Annex 1), que cal renovar periòdicament.

Les tecnologies actualment habilitades són les següents:

- RDP (escriptori remot): per a ús intern per accés a servidors
- VPN per a teletreball i accés a aplicacions i servidors des d'Internet
- Teamviewer (o alternatives – Anydesk, System Center, etc.) per al manteniment d'equips de treball i suport a l'usuari. Encara estem definint l'eina a fer servir.

4.3.3 Wifi

Els centres d'Aspace disposaran d'una xarxa inalàmbrica d'accés a la xarxa, per tal de:

- Solucionar mancances de la xarxa cablejada o facilitar la mobilitat dels professionals
- Oferir un servei addicional (accés a Internet) als usuaris d'un dels serveis d'Aspace

Hi haurà dues xarxes Wifi diferenciades:

1) **Treball (WORK-A-SPACE)**. Servirà per tal que els professionals accedeixin als recursos i a la informació interna d'Aspace. Les característiques específiques seran:
    - SSID ocult
    - Protegit amb contrasenya (s'especifica a continuació)
    - Estarà integrada dins de la xarxa de treball d'Aspace, i per tant permetrà l'accés a la informació dels servidors.
    - El departament TIC serà qui habilitarà la connexió a la xarxa de treball en els equips que siguin necessaris.

2) **Pública (ASPACE-WIFI)**. Servirà per donar accés a Internet a les persones que estiguin als centres d'Aspace.
    - SSID públic
    - Protegit amb contrasenya (s'especifica a continuació), diferent de la xarxa de Treball.
    - La contrasenya es facilitarà sota demanda, i en alguns casos (d'accés públic) es publicarà de forma visible.
    - No permetrà l'accés als servidors, només oferirà connexió a internet (amb una prioritat menor que la de la xarxa de treball).

En els casos en què hi hagi una xarxa Wifi activa, cal verificar el següent:

- El tipus de seguretat és WPA2-Personal
- El tipus d'encriptació és AES
- La contrasenya de la xarxa privada ha de tenir un mínim de 20 caràcters, i ha de contenir una combinació de:
    a. Caràcters (majúscules i minúscules)
    b. Números
    c. Símbols
- La contrasenya de la xarxa pública ha de tenir un mínim de 10 caràcters, que tinguin una combinació de:
    a. Caràcters (majúscules i minúscules)
    b. Números
    c. Símbols
- Aquestes dues xarxes Wifi es configuraran de la mateixa manera (SSID i contrassenya en tots els centres d'Aspace).
- La contrasenya ha de canviar-se cada any.
- En els casos en què l'objectiu de la Wifi sigui oferir accés a internet, la configuració de xarxa ha de restringir l'accés a aquest únic objectiu.

4.3.4 VPN

Donat que en el futur serà necessari realitzar connexions segures a la xarxa informàtica d'Aspace des de fora de la mateixa, tècnicament es preveu aquesta possibilitat considerant dues casuístiques concretes:

- **Personal d'Aspace itinerant**. És a dir, connexions d'usuaris a la xarxa d'Aspace per a treballar des d'un lloc alternatiu de forma segura. Cal preveure una certa flexibilitat de forma que la connexió es pugui efectuar des d'equips diferents i amb varietat d'horaris (VPN per software).
- **Connexions estables a sistemes externs**. En els casos en què calgui tenir un canal segur de comunicacions amb alguna altra entitat (exemple: HC3).

La connexió remota s'haurà de fer des d'equips propietat d'Aspace, que hauran d'haver estat preparats específicament pel departament de Sistemes. El nivell d'encriptació haurà de complir amb els requeriments definits en aquesta política.

4.3.5 Seguretat interna

En aquest apartat es defineixen les configuracions necessàries a nivell de la xarxa informàtica per tal d'evitar (o limitar) els accessos il·lícits a la informació.

Com a norma general, totes les opcions estaran restringides, i s'aniran habilitant permisos en funció de les necessitats.

Servidors i recursos compartits

Els servidors i dispositius annexes seran només accessibles en la seva globalitat pels administradors de la xarxa.

Als usuaris se'ls assignaran permisos (a aplicacions i recursos de xarxa) en funció de les seves necessitats. Aquestes necessitats s'agruparan en perfils genèrics per a facilitar l'administració de la xarxa.

Equips de treball

Els usuaris estaran habilitats per a fer servir els llocs de treball d'acord amb les seves necessitats. Com a norma general, no estaran habilitats com a administradors del seu equip ni podran realitzar modificacions de les configuracions, instal·lació d'aplicacions, etc. Qualsevol canvi haurà de ser autoritzat pel departament d'informàtica i executat per les persones autoritzades a aquest efecte.

Es bloquejarà l'execució automàtica de CDs i USBs per tal d'evitar la disseminació de virus. No s'estima necessari (de moment) la deshabilitació general de ports USB i altres dispositius (com

ara unitats de CD), ni la restricció de l'accés a Internet. Aquestes són opcions tècnicament factibles que poden ser implantades en un futur si s'estima necessari.

Els equips disposaran de les aplicacions necessàries per a les funcions requerides pel lloc de treball, que estaran homologades i correctament llicenciades d'acord amb la política tecnològica d'Aspace. En el cas de sorgir la necessitat d'alguna aplicació no homologada, el departament de sistemes en farà un estudi tècnic per tal de procedir, si s'escau, a la seva homologació i implementació.

Configuració de xarxa

Tots els ports i vies de comunicació interna no imprescindibles s'han de deshabilitar per a prevenir problemes. Qualsevol eina o aplicació que requereixi l'obertura d'algun d'aquests ports ha de ser aprovada pel departament de sistemes.

De la mateixa manera, els recursos de xarxa compartits s'han d'ocultar per defecte, permetent que siguin visibles només per a aquells usuaris amb els permisos requerits.

En la mesura del possible, la xarxa se segmentarà per tal de millorar la gestió del tràfic i les seves prestacions globals, a més de millorar la seguretat. Aquesta segmentació es podrà implementar de forma física (separant xarxes) o lògica (per mitjà de VLANs).

Polítiques de seguretat de nivell 2 i 3 (switch):

- Nivell 2:
    a. VLAN's
        i. Veu
        ii. Wifi
        iii. Operativa
        iv. Servidors
        v. Servidors DMZ
        vi. Backups
        vii. Administració
        viii. Nativa (1)
    b. QoS
        i. Priorització de paquets
- Nivell 3:
    a. Segments de xarxa

Monitorització

El departament de sistemes supervisarà i vetllarà constantment per la seguretat i la qualitat del servei dins de la xarxa d'Aspace. Es realitzarà una monitorització per tal de detectar:

- Intents d'accés a recursos no permesos (seguretat)
- Baixades de rendiment a la xarxa
- Falles de xarxa o de serveis
- Altres situacions no previstes

4.3.6 Anti-virus

Com a part molt específica de l'anterior punt, Aspace conta amb un programari anti-virus corporatiu instal·lat a totes els equips informàtics que ho requereixin (particularment, servidors i equips de treball).

Aquest programari compleix les següents premises:

- Instal·lació i gestió centralitzada
- Actualització diària centralitzada de les bases de dades d'amenaces
- Protecció en temps real
- Escanejos periòdics programats. Es realitza com a mínim un escaneig setmanal de tots els equips, i un escaneig diari en el cas dels servidors.
- Centralització dels avisos en cas de detecció d'amenaces o de mal funcionament de la plataforma.
- Firewall: bloqueig d'intents de connexió a l'exterior de programes no permesos (configuració centralitzada).

Els paràmetres de configuració del programari s'establiran d'acord amb l'especificat a l'Annex 8 - Parametrització anti-virus.

4.3.7 Política d'encriptació

En aquells casos que es requereix l'encriptació de la informació per tal de protegir-la d'accessos no autoritzats, el procediment i algoritmes emprats hauran de satisfer uns criteris de seguretat elevats (els màxims comercialment disponibles a un cost raonable).

En el cas d'Aspace, aquests criteris són:

- Algoritme d'encriptació AES de 256 bits (per exemple a l'hora d'encriptar fitxers).
- Sistemes de clau pública/clau privada RSA (per exemple per a VPNs),
- Accessos SSL (https) (per exemple per a aplicacions web).

4.3.8 Còpies de seguretat

Tota la informació d'Aspace ha d'estar protegida com a mínim per dos sistemes de còpies de seguretat: un de local i un de remot (que es descriu en el punt següent). L'objectiu és doble:

- D'una banda, estar protegit contra esborrats (accidentals o intencionats) o modificacions no desitjades de la informació. Cal guardar diferents versions dels documents i dades.
- D'altra banda, estar protegits contra falles del maquinari a on s'allotja la informació. Cal guardar còpies de forma que es pugui recuperar de forma ràpida l'activitat.

Pel que fa a la còpia local, cal fer almenys una còpia diària de tota la informació. Idealment se'n faran dues còpies diàries, i en el cas de la informació més crítica (com per exemple bases de dades d'aplicacions crítiques) caldrà mantenir una duplicació continuada de la informació (redundància).

Pel que fa als servidors, la configuració és la següent:

- Redundància de discos en màquines físiques: RAID-1 o RAID-5, de forma que el sistema suporti la falla d'un dels discos.
- Instantànies de windows: Permet crear punts de restauració del sistema i tornar a versions antigues de fitxers. Cal fer-ne un mínim de dos diaris (per defecte: 7:00 i 12:00).
- Còpia de seguretat del servidor: Realitza còpies a un disc extern (local) un o dos cops al dia.
- Els dispositius on es fa la còpia local s'ubiquen (tancats amb clau) en els mateixos racks a on estan els servidors.
- Les còpies generen un avís (correu electrònic) en el moment d'acabar-se per tal de poder monitoritzar el seu resultat i detectar problemes.

Periòdicament (cada sis mesos) cal fer proves de restauració de les còpies de seguretat. Tant de fitxers com de màquines senceres.

4.3.9 Còpies remotes

La llei de protecció de dades obliga a mantenir una còpia de la informació de nivell alt en una ubicació diferent dels repositoris originals, amb periodicitat mínima setmanal.

Addicionalment, i amb l'objectiu de tenir una cobertura contra fenòmens sísmics o d'un impacte territorial molt ampli, Aspace realitza internament aquestes còpies remotes, aprofitant l'existència de diferents centres. D'aquesta manera:

- La informació de tots els centres externs (CRA, CET, CTO Poble Nou i CIS Badalona) es tractarà de la forma següent:
    a. En els casos que sigui viable, la informació residirà a la vegada (de forma sincronitzada) tant en els centres com en la seu principal de Montjuïc, o residirà a Montjuic i serà accedida de forma remota des dels centres.

b. En els casos en què per la raò que sigui (volum excessiu, retards d'accés, etc.) la informació resideixi únicament en els servidors satèl·lit, es farà el següent:
    i. Còpia remota (via xarxa) de les carpetes amb dades de caràcter personal de nivell alt, amb periodicitat mínima setmanal.
    ii. Trasllat físic d'un disc de còpies de seguretat locals. En mesos alternatius s'utilitzaran dos discos de forma que es tingui una còpia total del servidor (d'una antiguitat màxima d'un mes) fora del local.

- La informació dels centres de Montjuïc (Centre Pilot, Escola, Residència) es copia a la vegada en els dos edificis de Montjuic (això ja compleix amb els requisits legals). Quan sigui tècnicament viable, i per major seguretat, es farà una còpia remota de la informació de Montjuïc en el centre del carrer Marc Aureli.

Aquestes còpies tenen les següents característiques:

- Com a mínim se'n fan còpies setmanals completes de tota la informació de nivell alt present als servidors, identificada per carpetes concretes.
- D'aquestes còpies se'n guarden 4 versions (l'equivalent a un mes), que es van esborrant a mesura que es guarden noves versions. Tanmateix, la primera còpia de cada mes es conserva durant 1 any de forma que existeixi un històric dels darrers 12 mesos.
- Les còpies s'emmagatzemem en equips i/o suports dedicats, a on només hi tenen accés els administradors del sistema.
- Pel que fa als dispositius que es traslladen, aquests estaran encriptats.
- Hi ha un procediment setmanal de revisió de l'execució correcta d'aquestes còpies.
- Periòdicament (cada 6 mesos) es realitzen proves de recuperació de la informació emmagatzemada.

4.3.10 Obsolescència i esborrat

La informació personal ha d'estar present i accessible en els sistemes d'Aspace al llarg de la relació entre l'entitat i la persona a qui fa referència, i en alguns casos s'ha de custodiar fins i tot després que s'hagi acabat aquesta relació. Els casos concrets amb els temps legals establerts estan inclosos a l'Annex 7 – Obsolescència de la Informació.

Mentre les dades no es considerin obsoletes, no es poden esborrar. En canvi es poden "inactivar" aquelles que es consideri que ja no són d'utilitat per a l'activitat normal, però que poden ser requerides per alguna raó (estudis estadístics, referència històrica, requeriments judicials, etc.). Aquestes dades inactives no seran accessibles mitjançant procediments estàndards, però restaran a l'abast dels administradors del sistema i/o persones amb permisos especials per al seu accés.

Un cop s'hagi declarat obsoletes les dades, s'haurà de procedir a la seva eliminació o esborrat (en funció del suport a on estiguin dipositades) d'acord amb el procediment de destrucció i esborrat de la informació (especificat en l'Annex 9).

En cas que una persona exerceixi el seu dret a la cancel·lació de les dades, es procedirà en funció del que es descriu en el procediment relatiu als drets ARCO, que s'especifica en un punt posterior d'aquesta política. En qualsevol cas, la cancel·lació de la informació no implica el seu esborrat o destrucció immediat. En funció dels requeriments legals d'obsolescència (reflectits a l'Annex 7 d'obsolescència) pot ser que calgui custodiar-la un temps determinat, però en tot cas no serà accessible per al seu ús.

4.3.11 Destrucció de suports informàtics

Tots aquells dispositius d'emmagatzemament que es deixin de fer servir (fins i tot aquells que no funcionin) s'hauran de destruir o esborrar abans de llençar-los, seguint el procediment de destrucció i esborrat de la informació (especificat en l'Annex 9). En cas de voler-los reciclar (ja sigui internament o externa) caldrà fer-ne un esborrat exhaustiu de tota la informació per tal d'impedir-ne al 100% l'accés a la informació que contenien.

4.4 Accés a la informació

A nivell de seguretat, els aspectes més rellevants són els que es descriuen en els punts següents. El fet que la informació es conservi i/o destrueixi adientment és una tasca específica del departament d'informàtica (per a les dades digitalitzades). El més important serà com i qui pot accedir i utilitzar aquesta informació. Els mitjans i polítiques per a controlar, monitoritzar i restringir aquests accessos són els que es descriuen a continuació.

4.4.1 Usuaris informàtics

L'accés als recursos informàtics d'Aspace es realitzarà per mitjà d'un codi d'usuari i una contrasenya que serviran per a identificar la persona que està accedint i registrar la seva activitat en la xarxa. Per tant aquests codis d'usuari són personals i intransferibles.

L'assignació d'aquests codis d'usuari i contrasenya es farà a requeriment del responsable de l'àrea o servei, la realitzarà el departament TIC i es notificarà en paper l'alta de l'usuari corresponent i la seva contrasenya inicial.

Els codis d'usuari (que en sí són dades personals que estan integrades al fitxer de recursos humans) es composaran d'acord amb el següent criteri general:

- La inicial del nom, o les inicials de cada nom en cas de ser un nom compost
- El primer cognom sencer
- En els casos que així s'originin usuaris redundants, s'optarà (per ordre) per les opcions següents:
    a. Afegir al final la inicial del segon cognom

b. Fer servir el nom sencer enlloc de la inicial del nom
c. Fer servir nom i cognoms sencers
d. Afegir un número seqüencial (1, 2, 3...) al final del codi d'usuari.

Aquesta mateixa norma s'aplicarà a les adreces de correu electrònic.

Casos particulars

- En alguns casos existeixen codis d'usuari no personalitzats (de departament o càrrec). Això també afecta a correus electrònics. Aquests casos han d'estar identificats i anotats en el Registre 9 - Llistat d'Usuaris i Correus departamentals, indicant quina és la persona (única) responsable de la gestió de l'usuari en qüestió. En cap altre cas es permet que hi hagi més d'una persona gestionant un codi d'usuari o una adreça de correu electrònic.
- Hi ha restriccions tècniques que poden imposar que un mateix professional gestioni més d'un codi d'usuari. Per tant, aquests codis d'usuari s'hauran de diferenciar d'alguna manera. Els casos concrets coneguts són:
    a. Usuaris de l'aplicació de visites per a consulta externa i per a CDIAP. Com que el codi d'usuari determina a quina base de dades s'accedeix, els usuaris que hagin d'accedir al CDIAP afegiran una lletra "c" al seu codi d'usuari normal.
- En algunes ocasions pot ser necessari posar un codi d'usuari personals que no es correspongui al nom i cognom de la persona. Per exemple, en el cas d'un usuari d'un centre que té un cognom molt llarg i difícil d'escriure s'opta per posar un codi curt i senzill (tot i que a la definició de l'usuari dins del domini d'Aspace sí que se li posa el nom complert).

En la mesura que tècnicament sigui possible, sempre es faran servir un únic codi d'usuari (emmagatzemat i gestionat centralitzadament) per a tots els serveis d'Aspace. Per a fer-ho s'implementaran tecnologies "Single Sign On" i d'integració LDAP. Aquest requeriment s'haurà de considerar per a les implementacions de noves eines i serveis.

Àmbits dels usuaris: Inicialment no totes les aplicacions informàtiques d'Aspace comparteixen els codis d'usuari. En particular, existeix la següent diferenciació:

- **Usuaris de domini**: Aquells que es fan servir per a autentificar-se i iniciar la sessió a l'equip de treball, connectant-se a la xarxa local.
- **Usuaris d'aplicació**: Aquells que s'utilitzen per a accedir a la informació disponible en les aplicacions d'Aspace, ja sigui des de dins de la pròpia xarxa com des de fora d'ella (via Internet) en aquells casos en què aquesta opció estigui habilitada.

A mesura que tecnològicament sigui viable (per a les aplicacions pre-existents) i com a pre-requisit (per a les noves), caldrà tendir a que cada persona tingui un únic usuari, que es farà servir per a identificar-se en tots els serveis i aplicacions informàtiques.

4.4.2 Bloqueig per reintents

Com a norma general s'establirà un límit d'intents d'accés erronis consecutius, de forma que es permetrà un màxim de 10 intents erronis. En cas de superar-se aquest límit, l'usuari es bloquejarà i no es permetrà l'accés a l'entorn o a l'aplicació.

El desbloqueig es produirà automàticament després d'un mínim de 30 minuts, tot i que en funció del tipus d'aplicació, es pot establir que aquest bloqueig sigui permanent fins que els administradors realitzin el procés de desbloqueig.

4.4.3 Política de contrasenyes

Les contrasenyes dels usuaris d'Aspace hauran de complir els requisits següents:

- Complexitat:
    a. Han de tenir un mínim de 8 caràcters.
    b. Han de contenir lletres majúscules i minúscules, números i símbols.
- Les contrasenyes caduquen cada 6 mesos. El sistema avisarà uns dies abans.
- En renovar contrasenyes, no es podrà repetir fins a 14 contrasenyes prèvies.
- S'emmagatzemen en camps encriptats, de manera que els administradors no hi tenen accés.

Aquests requeriments, que són vàlids tant per a l'accés als recursos de xarxa com a les diferents aplicacions i webs corporatives, estaran configurats a nivell d'administració i per tant no es deixaran a l'arbitri dels propis usuaris.

Com s'ha comentat en altres punts, les contrasenyes són confidencials i no es poden compartir ni cedir a d'altres usuaris.

Excepcions a aquestes normes:

- **Usuaris d'administració**: Són codis d'usuari que sovint es configuren en llocs clau de la parametrització de les eines informàtiques, i a més tenen una capacitat molt superior per a causar problemes de seguretat. Tanmateix, no es fan servir de forma habitual per a accedir als sistemes i/o informació. Per tant:
    a. La complexitat de la contrasenya serà superior:
        i. Mínim 15 caràcters.
        ii. Han de contenir lletres majúscules i minúscules, números i símbols.
    b. Sí es permetrà la compartició de la mateixa entre les persones que realitzin tasques d'administració, tot i que en general serà preferible utilitzar usuaris "personals" amb permisos administratius per tal d'evitar accessos "anònims".

    c. La contrasenya no canviarà com a norma general perquè no són usuaris que es facin servir per accedir a la informació, sinó per modificar paràmetres d'administració.
- **Persones usuàries de centres i serveis d'Aspace**: Solen ser persones amb majors o menors limitacions intel·lectuals, i que suposen un risc molt reduït de seguretat pel seu accés molt limitat a la informació. Per tant:
    a. La seva contrasenya no tindrà requisits de complexitat.
    b. La seva contrasenya serà coneguda per les persones (monitors, professors) que en són responsables.
    c. La seva contrasenya no caducarà.
- "**1234**": Codi d'usuari genèric per a accedir a l'ordinador per a les persones usuàries dels serveis d'Aspace. No té contrasenya, però no permet accedir a cap dels repositoris de dades d'Aspace.
- "**adaptat**": Semblant a l'anterior, usuari sense contrasenya que es fa servir al servei de l'escola. Sí que té permisos per accedir als servidors, però únicament a una carpeta a on s'emmagatzemen perfils dels diferents usuaris dels serveis d'Aspace, per a aplicacions adaptades a les seves necessitats personals (exemple: perfils de comunicació). Aquest accés no està implementat i per tant només és conegut pel personal informàtic d'Aspace.

Assignació i distribució de contrasenyes

Els administradors seran els encarregats de generar la contrasenya inicial de tots els usuaris amb accés als sistemes d'Aspace. En el cas d'haver de crear més d'un usuari per a aplicacions o recursos diferents, el procediment serà el mateix tot i que sempre s'intentarà fer-ho de forma simultània per tal d'entregar d'un sol cop a l'usuari totes les eines que necessita.

El procediment concret un cop s'ha creat l'usuari serà:

1. S'assigna una contrasenya inicial que compleixi els requeriments de seguretat.
2. Sempre que els sistemes ho permetin, es marca l'usuari per tal que obligatòriament canviï la seva contrasenya el primer cop que accedeixi al sistema.
3. Es comunica formalment al nou usuari la disponibilitat del codi d'usuari i la contrasenya inicial, així com la necessitat de canviar-la d'immediat. Això es fa mitjançant l'entrega d'un document a on figuren les credencials d'accés als recursos. Aquest document es pot:
    - Entregar en mà al nou usuari, o
    - Entregar a Recursos Humans per tal que el facin arribar al nou usuari en el moment que s'incorpori.

En el cas de sistemes que no permetin forçar el canvi de contrasenya en el primer login, es requerirà que sigui el nou usuari qui es posi la contrasenya de forma presencial.

En cas que l'usuari oblidi o perdi la contrasenya per accedir als serveis es procedirà a restablir-li la contrasenya seguint el procediment previ. No obstant, en casos de sistemes que admetin forçar el canvi de contrasenya en el primer login es permetrà que la comunicació de la contrasenya temporal es faci per via telefònica sempre que l'interlocutor sigui directament l'usuari a qui se li està restablint.

En cap cas es transmetrà una contrasenya per correu electrònic de forma conjunta al codi d'usuari. La preferència serà sempre fer servir el canal telefònic o el format paper.

En cap cas el departament TIC portarà un registre de les contrasenyes assignades als usuaris, exceptuant els comptes d'usuaris administradors (que són utilitzades exclusivament pel propi departament TIC).

4.4.4 Assignació de permisos

Els usuaris i els seus perfils determinaran els permisos bàsics necessaris per a accedir a la informació. Tanmateix, si cal que algun usuari tingui permisos concrets addicionals als que li pertoquen d'acord amb el seu perfil, caldrà una aprovació explícita per part del seu directors o responsable. I en cas que aquests permisos addicionals impliquin accés a dades de caràcter personal, caldrà una autorització per part del responsable del fitxer corresponent.

Perfils bàsics:

- **Superadministrador**: Codis d'usuari de caràcter tècnic, no associats a persones concretes, i amb permisos per administrar tota la plataforma. Es fan servir per a fer parametritzacions que necessiten d'aquests permisos i per a les quals no s'han de canviar les contrasenyes de manera periòdica. No s'ha de fer servir per al manteniment o l'administració dels sistemes (per a això ja estan els usuaris administradors).
- **Administradors**: En general són els usuaris que tenen l'encàrrec d'administrar la plataforma. Disposen d'un nivell d'accés alt a tota la informació (de forma directa o bé se'n poden configurar l'accés).
- **Usuaris avançats**: Són els usuaris que tenen algun tipus de control sobre la parametrització dels sistemes, o sobre altres usuaris, sense ser administradors. No tenen més permisos d'accés a la informació que els que se'ls assignin, i no se'n poden configurar més per ells mateixos.
- **Usuaris**: Són els estàndards. Estan molt limitats quan a la seva capacitat de configuració de l'entorn i accés a la informació. Només poden fer allò per al que se'ls dóna permís.
- **Nois**: Són els usuaris amb menys permisos, pensats per a que les persones usuàries dels centres d'Aspace puguin accedir a Internet o a determinades carpetes de xarxa específicament dedicades per a ells.
- **Codis d'usuari auxiliars**: No estan assignats a persones, i serveixen per a desenvolupar tasques específiques de sistemes, amb permisos molt limitats d'acord amb aquestes

tasques. Les seves credencials són conegudes únicament pels administradors de sistemes.

El personal del departament TIC encarregat del manteniment de la plataforma disposarà de dos tipus d'usuaris personalitzats:

- L'usuari estàndar, de perfil "usuari" o "usuari avançat", que li servirà per a la feina del dia a dia.
- L'usuari administrador, de perfil "administrador", que li servirà per a administrar la plataforma.

Un llistat més complert dels diferents perfils definits es pot trobar a l'Annex 10 - Perfils d'usuari.

Processos d'assignació i modificació de permisos (informàtics)

1) Alta de l'usuari

- Responsable: Sol·licitud de la creació d'un nou usuari per a accedir al sistema. Aquesta sol·licitud contindrà la informació següent:
    i. Persona responsable que autoritza l'alta
    ii. Dades del nou usuari (nom i cognoms)
    iii. Lloc de treball i perfils associats
    iv. Recursos informàtics estàndard necessaris (lloc de treball, email, xarxa, aplicacions, etc.)
    v. Necessitats especials (accés no estàndar a informació, accés remot, dispositius mòbils, etc.)
- TIC: Creació de l'usuari o usuaris necessaris i assignació dels perfils de seguretat i contrasenyes inicials. Parametrització dels equips.
- TIC: Documentació de les accions realitzades (si cal)
- TIC: Comunicació de l'alta a la persona responsable

2) Modificació de l'usuari

- Responsable: Sol·licitud de l'alteració dels permisos d'un usuari existent per a accedir al sistema. Aquesta sol·licitud contindrà la informació següent:
    i. Persona responsable que autoritza la modificació
    ii. Dades de l'usuari (nom i cognoms o codi d'usuari)
    iii. Motiu canvi (canvi de lloc de treball, canvi de funcions, etc.)
    iv. Canvi de perfils
    v. Recursos informàtics estàndar necessaris (lloc de treball, email, xarxa, aplicacions, etc.)
    vi. Necessitats especials (accés no estàndar a informació, accés remot, dispositius mòbils, etc.)

- TIC: Creació o modificació de l'usuari o usuaris necessaris i assignació dels perfils de seguretat. Reparametrització dels equips necessaris.
- TIC: Documentació de les accions realitzades (si cal)
- TIC: Comunicació de l'alta a la persona responsable

3) Baixa de l'usuari

Aquest és un procés molt important que cal estandaritzar a nivell de l'organització. El departament TIC no sap quan una persona causa baixa, i per tant no pot iniciar el procés per si sol.

- Responsable: Sol·licitud de baixa d'un usuari existent. Aquesta sol·licitud contindrà la informació següent:
    i. Persona responsable que autoritza la baixa
    ii. Dades de l'usuari (nom i cognoms o codi d'usuari)
    iii. En cas necessari, persona o usuari a qui s'assignen els permisos al lloc de l'usuari que causa baixa.
    iv. Data efectiva de la baixa en els diferents recursos i serveis.
    v. Previsió de temps de baixa (si aquesta és temporal)
- TIC: Desactivació dels usuaris requerits i parametrització dels usuaris que han d'accedir a la informació en el seu lloc, si cal.
- TIC: Reclamació del retorn dels equips i dispositius de l'usuari.
- Responsable: Retorn a TIC (un cop la baixa ja sigui efectiva) dels equips i dispositius de la persona que causa baixa.
- TIC: Esborrat de la informació associada a l'usuari que causa baixa en els equips i dispositius, i preparació per a la seva assignació a d'altres usuaris.
- TIC: Documentació de les accions realitzades (si cal)
- TIC: Comunicació de la baixa a la persona responsable

4.4.5 Plataforma informàtica

La plataforma informàtica d'Aspace està formada per tots aquells equips (PCs i altres dispositius) que són propietat d'Aspace i que fan servir els professionals i voluntaris per realitzar les seves tasques i accedir a la informació corporativa.

Donat que els recursos són limitats, els equips s'han de fer servir exclusivament per a finalitats relacionades amb els serveis d'Aspace.

Quan tècnicament sigui viable, els equips es configuraran i gestionaran de forma centralitzada (en domini), de forma que aquesta gestió sigui automatitzada i el més òptima possible.

4.4.5.1 Nomenclatura i etiquetat dels equips i dispositius

Tots els equips tindran un identificador únic, que serà el mateix a nivell de xarxa i a nivell físic. Aquest identificador s'establirà d'acord amb l'especificat a l'Annex 6, i s'aplicarà a l'equip corresponent de la forma següent:

- A nivell físic, s'etiquetarà l'equip amb el seu identificador en un lloc extern visible.
- A nivell lògic, es posarà l'identificador com a nom de màquina.

4.4.5.2 Configuració bàsica dels equips de treball

Tots els equips tindran una configuració bàsica homogènia per tal de permetre la flexibilitat dels punts de treball. Aquesta configuració, que es detalla en l'Annex 11 - Model tecnològic del lloc de treball, serà definida, actualitzada i implementada per l'àrea d'informàtica, i inclou els següents aspectes:

- Maquinari: Equips informàtics, de telefonia, dispositius, etc.
- Programari: Sistema operatiu, instal·lació d'aplicacions, etc.
- Mobilitat: Parametritzacions necessàries per a l'accés a la informació corporativa des de llocs alternatius de treball (si s'escau).

Els usuaris no tindran en general permisos administratius en els seus equips ni dispositius, de forma que no es podran instal·lar noves aplicacions ni modificar la configuració del sistema (cosa que és responsabilitat dels administradors de la plataforma). En cas necessari l'administrador de sistemes podrà decidir donar permisos d'administració a un usuari en algun dels casos següents:

- En cas de necessitat tècnica per a executar una aplicació que requereixi permisos d'administració.
- En el cas que per la pròpia feina i responsabilitat de l'usuari tingui autorització per a instal·lar aplicacions.

4.4.5.3 Requeriments en matèria de seguretat

En particular, per tal de donar resposta als requeriments legals en matèria de protecció de dades personals, caldrà configurar els següents aspectes:

- Protecció amb contrasenya per iniciar la sessió.
- Bloqueig de pantalla automàtic per inactivitat: 10 minuts
- En el cas dels PCs, requerir prémer la combinació de tecles Control+Alt+Supr per a iniciar la sessió o desbloquejar la pantalla.

- Encriptació automàtica de les dades en el cas de dispositius portàtils. Depenent de la necessitat d'informació, es podrà realitzar una encriptació total del dispositiu, o generar un "espai o unitat encriptada" en el mateix.
- Bloqueig de l'execució automàtica de dispositius externs.
- No es contempla inicialment la deshabilitació de potencials vies de "fuga" d'informació, però pot ser que sigui necessari fer-ho en un futur:
    a. A dispositius externs: USB, CDs, etc.
    b. Via Internet

Existeixen algunes excepcions a aquestes normes (en general descrites en altres àmbits de la present política). Les més rellevants són:

- Equips destinats a persones usuàries de centres i serveis d'Aspace (amb necessitats especials d'accessibilitat). En aquests casos:
    a. Es permetrà l'accés amb l'usuari "1234" (que no té contrasenya, i no permet l'accés a dades).
    b. No es requerirà la combinació de tecles Control+Alt+Supr per iniciar sessió o desbloquejar l'equip.

4.4.5.4 Mapeig de carpetes

De manera predefinida els usuaris tindran accés a les carpetes de xarxa que els pertoquin, estiguin en el centre que estiguin, sempre que inicïin la sessió amb el seu usuari del domini. Aquestes carpetes estaran mapejades seguint el següent criteri:

Lletres d'unitat	Situació actual	Descripció ús
C: a K:	Actiu	Unitats locals (discos durs, USB, lectors de targetes, etc.)
L:	Reservat	Mapeig d'arxius PST (si s'escau)
M:	Actiu	Carpeta encriptada (en els equips que estigui aquesta opció)
N:	Reservat	Carpeta personal
O:	Reservat	Programa FundaSoft
P:		
Q:		
R:	Actiu	Reservat aplicacions (The Grid)
S:		
T:		
U:		
V:		
W:	Actiu	Carpeta de mapeig de dades de servei (principal)
X:		
Y:		
Z:		

El llistat detallat del mapeig que correspon a cada perfil d'usuari s'inclou en l'Annex 10.

4.4.6 Desenvolupament i proves d'eines informàtiques

En totes aquelles aplicacions i sistemes que estiguin allotjades als servidors d'Aspace es mantindran dos o tres entorns diferents per tal de minimitzar riscos de pèrdua d'informació i restringir-ne al màxim l'accés a les persones que s'encarreguen de mantenir-los i desenvolupar-ne noves funcionalitats.

Aquests entorns són els següents:

- **Desenvolupament**: Entorn sense dades reals a on hi poden accedir lliurement les persones encarregades de fer la codificació de les noves funcionalitats.
- **Integració/Test**: Entorn amb dades reals dissociades, pensat per semblar-se el màxim possible a l'entorn de producció. Hi han de poder accedir tant els desenvolupadors com els usuaris (testejadors) de les aplicacions. En alguns casos, si la dimensió de l'aplicació no ho justifica, es pot prescindir d'aquest entorn.
- **Producció**: Entorn a on resideixen les dades reals. Només hi poden accedir els usuaris d'acord amb els perfils i permisos especificats, i els administradors de sistemes per al seu manteniment.

El detall d'aquests entorns, així com els procediments associats a la gestió de les dades i de les versions, i els aspectes de qualitat i seguretat en el desenvolupament es troben en l'Annex 18, de desenvolupament d'aplicacions.

4.4.7 Entrega d'informació

La norma general és que la informació corporativa d'Aspace resideix en els repositoris descrits anteriorment, i és allà a on es realitzen accessos i es manté aquesta informació (evitant duplicitats i possibles incoherències).

No obstant això, hi ha alguns supòsits en els què pot ser necessari extreure una còpia de la informació corporativa per a entregar-la a persones alienes a l'organització. Aquests supòsits són:

- **Facturació**. Generació de factures a administracions o usuaris dels serveis (pot ser necessari incloure llistats d'usuaris, serveis facturats, etc.).
- **Entrega d'informes mèdics**. Qualsevol informació de caràcter mèdic referent a un dels usuaris dels serveis d'Aspace que sigui requerida en qualsevol àmbit (escola, CAP, hospital, serveis de lleure, etc.) se li entregarà sempre a l'usuari en persona o al(s) seu(s) representant(s) legal(s) en cas de ser menor d'edat o legalment incapacitat.
- **Entrega d'altres informes**. La resta d'informació (social, educativa, etc.) es vehicularà també a través dels usuaris o de les seves famílies.

- **Connexions a aplicacions externes**. En alguns casos la informació propietat d'Aspace pot estar integrada o sincronitzada amb aplicatius no allotjats en els servidors d'Aspace. En aquests casos, els processos de sincronització s'entendran com entrega de la informació corporativa cap a ens externs. Alguns d'aquests casos són:
    a. **RRHH**: Cezanne, Seguretat Social, etc.
    b. **HC3**: Història clínica compartida
- **Requeriments administratius o judicials.** En cas d'haver una petició degudament justificada, es podrà transmetre la informació requerida mitjançant els procediments definits en aquesta política.
- **Drets ARCO**. Aquest supòsit ja es descriu en el punt específic.

4.4.8 Política de registre d'accessos

La LOPD obliga a fer un registre d'accessos als fitxers (informàtics o no) de nivell alt. Cal guardar la informació necessària per identificar el registre accedit i saber si s'ha modificat o no, però no cal determinar el contingut modificat. En el cas dels arxius no informatitzats, no cal guardar un registre dels accessos per part de les persones que controlen i utilitzen l'arxiu de forma habitual (que són les persones autoritzades pel responsable del fitxer).

La informació mínima a emmagatzemar en el cas dels fitxers informatitzats serà per tant:

- **Usuari** que realitza l'accés: Codi que permeti identificar unívocament la persona que ho fa (i en el cas d'accessos informàtics, si és possible l'equip des del que s'accedeix).
- **Data i hora** d'accés: Moment exacte de l'accés.
- **Resultat** de l'accés: Si s'ha permès o no l'accés.
- **Tipus** d'accés**:** Lectura o modificació
- **Via** d'accés: Aplicació (i pantalla si s'escau)
- **Dades accedides**:
    a. **Fitxer:** Segons LOPD.
    b. **Registre:** Codi de la persona accedida.

Aquesta informació caldrà emmagatzemar-la durant dos anys.

A banda, es necessari fer-ne una anàlisi mensual per a detectar possibles problemes de seguretat. Per tant, serà important tenir un sistema de registre el màxim de centralitzat i automatitzat possible.

4.4.8.1 Accessos físics

Per als fitxers amb dades de nivell alt en suport físic (exemple, les dades de les històries clíniques) cal registrar aquells accessos físics a la ubicació on es troben les dades per part de persones que no en són les expressament autoritzades a fer-ho. El format concret d'aquest registre (anomenat

Registre 2 d'Accessos físics a repositoris), així com la seva ubicació es troba descrit a l'Annex 1 – Registres.

Al Registre 1 (Registre de repositoris) existeix una relació de persones autoritzades a accedir a les dades dels fitxers en format no automatitzat, sempre autoritzades pels responsables de fitxers.

4.4.8.2 Accessos informàtics

Totes les aplicacions i programes que permetin accedir a la informació han de guardar un registre d'aquests accessos, que sigui fàcilment accessible i explotable de cara a l'anàlisi posterior.

En particular, a nivell dels servidors centrals i de la xarxa de servidors de fitxers hi ha establerta una política que automatitza la recollida d'informació de registre al voltant de tres eixos:

- Accés a la xarxa (intents de login)
- Accés a la informació de la xarxa (navegació, obertura de fitxers, còpies, esborrat d'informació, etc.)
- Accés a la configuració de seguretat (intents de modificació de la pròpia política)

Aquesta política es descriu en detall en l'Annex 3, i correspon a la GPO de registre d'accessos.

Aquests tres eixos s'apliquen també al registre d'accessos de cada aplicació que així ho requereixi (particularment les que maneguen dades de nivell alt).

4.4.8.3 Patrons d'accés restringits (a controlar)

De cara a l'anàlisi mensual del registre d'accessos, es defineixen els següents patrons a detectar:

- **Intents d'accés denegats**. Poden indicar intents d'accés fraudulent, i servir per detectar vulnerabilitats de seguretat, entre d'altres.
- **Esborrat d'informació**. Pot ser una acció malintencionada, o accidental. Inclou una modificació d'informació que en redueixi el volum.
- **Accessos a la mateixa informació per persones diferents**. En alguns casos pot indicar accessos indeguts.
- **Accessos simultanis a la informació**. Pot servir per detectar infraccions en la política de contrasenyes (per exemple en cas d'accés simultani des d'equips diferents).

5 Registre d'incidències de seguretat

ASPACE mantindrà un llistat dels incompliments o mancances de seguretat que es detectin i que afectin a qualsevol punt de la present política o fins i tot a aspectes que no s'hi reflecteixin però que suposin amenaces per a la seguretat de la informació.

Aquestes situacions, denominades "incidències de seguretat" quedaran anotades en el Registre 5 d'incidències de seguretat, que es descriu en l'Annex 1 de registres.

Els objectius d'aquest registre seran:

- Assegurar el compliment de la LOPD i dels criteris de seguretat establerts a ASPACE.
- Detectar i identificar possibles mancances en la present política, o incompliments de la mateixa.
- Registrar les actuacions fetes per a resoldre les incidències de seguretat.
- Proposar millores en matèria de seguretat.

Aquest registre serà gestionat pels Responsables de Seguretat i mensualment se'n farà una revisió per a detectar les vulnerabilitats i establir un pla d'acció –en cas necessari- per a evitar aquestes vulnerabilitats.

Existeix un procediment per a la notificació i tramitació d'incidències que s'acompanya com a Annex 14 – Gestió d'incidències de seguretat.

5.1 Definició d'incidències de seguretat

Seran incidències de seguretat qualsevol succés que pugui donar lloc a les següents situacions:

- Pèrdua de privacitat de la informació.
- Registre per a la integritat de los dades.
- Accés i ús no autoritzat de serveis i sistemes.
- Bloqueig/Desbloqueig d'identificadors d'usuari.
- Modificacions no autoritzades d'informació.
- Denegació de servei.
- Incidències en la gestió de xarxa (caigudes de xarxa, servidors, comunicacions...).
- Errors del sistema/transaccions/bases de dades/usuaris.
- Mal funcionament durant la realització de còpies de seguretat.
- Recuperació de dades a partir de còpies de seguretat.

6 Procediments periòdics de control

6.1 Informes mensuals

El Responsable de Seguretat revisarà cada mes la informació de control registrada i el funcionament del sistema, i s'encarregarà d'elaborar un informe de les revisions realitzades i dels problemes detectats, proposant les accions correctores pertinents.

Aquest informe es farà arribar a l'Equip Directiu d'ASPACE i en particular als Responsables de Fitxer implicats en les conclusions, de forma que decideixin les accions a realitzar.

6.2 Proves semestrals de recuperació d'informació

Dues vegades l'any es realitzaran uns procediments de verificació del funcionament del sistema de còpies de seguretat, amb independència que s'hagin hagut de fer recuperacions d'informació en algun moment al llarg del període.

Aquestes proves hauran de verificar els sistemes més crítics, així com els procediments més estàndards a realitzar, per tal de:

- Assegurar el correcte funcionament del sistema de recuperació quan arribi el moment
- Conèixer i dominar els procediments necessaris per tal de poder-los efectuar amb més agilitat si es dóna el cas.

El procediment de realització d'aquestes proves es recull a l'Annex 16.

6.3 Auditoria bianual

Els sistemes d'informació i instal·lacions per al tractament de les dades estan sotmesos a una auditoria interna o externa, que verifiqui el compliment dels procediments i instruccions vigents referents a la seguretat de les dades, com a mínim cada dos anys. L'auditoria es fa a petició del Responsable del Fitxer, i aquest serà qui designarà a l'auditor o auditors corresponents.

L'objectiu d'aquesta auditoria és verificar i assegurar el compliment dels requeriments legals establerts en matèria de seguretat, així com detectar mancances i àrees de millora en aquest àmbit.

L'auditoria ha de contemplar, com a mínim, els punts següents:

- Identificació de les deficiències en matèria de seguretat de la informació de caràcter personal de les instal·lacions, sistemes d'informació, normatives, procediments i relacions amb tercers. Els controls actuaran bàsicament en les següents àrees:
    - Anti-malware dels equips i servidor
    - Sistema de gestió d'accessos
    - Sistemes d'identificació i autenticació
    - Compliment de les normes de confidencialitat i secret
    - Compliment dels fluxos d'informació als usuaris i al personal que cedeix les dades
    - Procediments de gestió de suports
- Establiment de mesures i recomanacions per a resoldre les deficiències detectades.
- Inclusió de les dades, fets i observacions en què es basen els dictàmens i recomanacions proposades.

El Responsable de Seguretat generarà un informe de conclusions resum per al Responsable del Fitxer o Tractament per tal que prengui les mesures correctores adequades. Les auditories i els informes de conclusions es dispositaran i arxivaran conjuntament amb els Documents de Seguretat.

7 Responsabilitats dels usuaris i treballadors d'Aspace

7.1 Deure de secret

Tots els treballadors d'Aspace tenen l'obligació de mantenir la confidencialitat sobre les dades i informacions a les que tinguin accés en funció de la seva feina, fins i tot un cop han acabat la relació laboral amb Aspace. Això és especialment important pel que fa a les dades mèdiques i de salut dels pacients i usuaris dels serveis d'Aspace.

Aquesta obligació de confidencialitat queda recollida en el **"Full d'Informació i Compromís de l'Empleat"** del personal en nòmina, inclós a l'Annex 4. Al personal se li fa entrega de la **"Guia de Bones Pràctiques**", on es detallen les instruccions a seguir per tots els usuaris amb accés a dades de caràcter personal.

7.2 Compliment de les polítiques

Tots els treballadors i qualsevol altre persona amb accés a les dades d'Aspace (voluntaris, usuaris, etc) haurà de complir (i fer complir) les polítiques descrites en aquest document, que es recolliran en la normativa interna corresponent.

7.3 Bon ús de les eines i aplicacions

D’acord amb els punts anteriors de la present política i per resumir:

- Utilitzar els equips i dispositius per a fins professionals
- Seguir les indicacions i procediments establerts
- Informar quan es detecti algun punt a millorar

7.4 Vetllar per la informació i denunciar incidències de seguretat

Les persones que tracten amb les dades d’Aspace han de responsabilitzar-se de les mateixes i vetllar per la seva seguretat, evitant les situacions de risc i assegurant que aquestes dades tornen al seu repositori corresponent al final del tractament, si és el cas.

De la mateixa manera, qualsevol treballador que detecti una situació que amenaci la seguretat i/o integritat de la informació ha d’informar-ho al Responsable de Seguretat a la major brevetat possible.

7.5 Sancions en cas d’incompliment

El no compliment de qualsevol de les polítiques i responsabilitats aquí descrites es considerarà com una infracció per desobediència de les normes internes d’ASPACE i donarà lloc a una falta.

Tota falta comesa per un/a treballador/a es classificarà com a lleu, greu o molt greu segons el conveni col·lectiu d’aplicació o la normativa de l’Estatut dels Treballadors i s’aplicaran les mesures disciplinàries atès el grau de les faltes.

8 Drets de les persones de les quals Aspace té dades personals

8.1 Drets ARCO

Els interessats inclosos en els fitxers tenen el dret d'accés, de rectificació, cancel·lació i oposició a les seves dades de caràcter personal, mitjançant sol·licitud al Responsable del Fitxer. Aquest passarà la sol·licitud al Responsable de Seguretat per tal que la pugui tramitar com més aviat millor.

Legalment s'han d'acomplir els terminis (accés: 1 mes, rectificació i cancel·lació: 10 dies). És molt important controlar que es doni resposta i complir els terminis establerts. S'han de tenir evidències dels lliuraments, fulles d'autoritzacions, etc, en cas que s'exercitin els drets.

Els casos ARCO que se surtin de la normalitat o que no s'hagin tramitat correctament, s'hauran de tractar en el comitè de seguretat per donar una òptima resposta.

A l'Annex 5 es detallen tots els aspectes relatius a l'exercici d'aquests drets, els models de sol·licituds, així com el procediment que per poder-los exercitar.

8.2 Dret de queixa

Tota persona que consideri que l'entitat ha actuat incorrectament en el tractament de les dades personals incloses en els diferents fitxers de DCP podrà dirigir-se al Responsable de seguretat, identificant-se de manera suficient i exposant per escrit el contingut de la queixa.

9 Responsabilitats

9.1 Definició de la política

Correspon a l'Equip Directiu d'Aspace la definició, esmena, aprovació i supervisió de la present política. En particular, les persones designades com Responsables de Fitxer d'acord amb la normativa vigent en matèria de protecció de dades personals són les responsables de tots els aspectes de seguretat que els corresponen legalment.

9.2 Implementació i compliment

Les persones responsables d'implementar i fer complir la present política són les següents:

Persona/Dept	Àmbit de responsabilitat
Direcció assistencial, Direcció pedagògica i Direcció de serveis comunitaris	Tots els protocols i procediments relacionats amb els usuaris dels serveis d'Aspace.
Direcció de recursos humans	Tots els protocols i procediments relacionats amb els treballadors i voluntaris d'Aspace.
Àrea TIC	Tots els elements tecnològics presents en aquesta política.
Responsables de seguretat	Supervisió de la implementació. Seguiment continuat.

S'inclou com annex un llistat detallat de responsables de la implementació de les polítiques descrites en el present document (Annex 12).

9.3 Responsable de Fitxer

D'acord amb el que estableix la LOPD, el Responsable de Fitxer és ASPACE, representat en cada un dels fitxers per la persona que es detalla en l'Annex 0. Aquesta persona és qui decideix sobre la finalitat, el contingut i l'ús del tractament dels fitxers de dades de caràcter personal de l'Entitat.

Pel que fa als fitxers de dades de caràcter personal dins del seu àmbit, el Responsable de Fitxer té les responsabilitats següents:

- Fer efectives les mesures de seguretat que es descriuen en aquest document
- Supervisar totes les funcions que afectin al tractament de les dades de caràcter personal
- Sancionar els incompliments

Tot i poder delegar les seves funcions en les persones que estimi convenient, la responsabilitat sempre és seva.

9.4 Responsable de Seguretat

El Responsable de Seguretat és l'encarregat de coordinar i gestionar les mesures de seguretat determinades a la Política de Seguretat. ASPACE designa com a responsables de seguretat a:

- Yolanda Elipe
- Paul Mussach

9.4.1 Funcions del Responsable de Seguretat

- Redactar i mantenir actualitzat els Document de Seguretat dels fitxers declarats a l'AEPD.
- Verificar periòdicament que l'inventari de fitxers de dades de caràcter personal de l'Entitat estigui actualitzat (veure l'Annex 0).
- Coordinar i controlar el compliment de les mesures de seguretat.
- Supervisar el Registre d'Incidències de Seguretat i controlar el llistat d'Incidències TIC que afecten a la seguretat.
- Revisió mensual dels Registres i del sistema de protecció de dades.
- Elaboració de l'Informe mensual de revisió del sistema.
- Anàlisi dels informes d'Auditoria propis i dels Encarregats de Tractament (si s'escau) i elevar-los al responsable del fitxer.
- Revisar els nous contractes amb proveïdors (tal i com s'estableix a l'Annex 22, de procediment de revisió de contractacions) per validar que compleixen amb els requeriments de protecció de dades i identificar la necessitat d'establir contractes d'encarregats de tractament o compromís de confidencialitat.
- Exigir el compliment de les condicions de seguretat a tots nivells quan el tractament el realitzi un tercer, mitjançant l'elaboració de compromisos legals amb els encarregats externs de tractament.
- El Responsable de Seguretat podrà delegar les seves funcions en el personal que estimi convenient, sempre que aquest estigui capacitat per portar a terme de forma efectiva les tasques encomanades, i sempre fent la corresponent menció en la present política. No obstant, no es delegarà la responsabilitat, la qual continuarà sent de la persona designada com a Responsable de Seguretat.
- Oferir suport i formació en matèria de Seguretat a tota l'organització.

9.5 Encarregats de tractament

És aquella persona física o jurídica que tracta dades personals per compte d'ASPACE. La relació jurídica amb l'encarregat extern del tractament haurà de ser regulada mitjançant el corresponent contracte per escrit, que inclourà les clàusules definides segons l'Annex 13 – Clàusules encarregats de tractament. A més ASPACE, en la mesura que pugui, sol·licitarà certificats de compliment de la normativa relativa a la protecció de dades.

Les seves obligacions són garantir el compliment de les mesures establertes en la Política de Seguretat i els diferents Documents de Seguretat, així com les derivades de la normativa aplicable, i respectar totes les condicions contractuals que el vinculin amb ASPACE. ASPACE es reservarà la potestat de requerir un certificat als Encarregats de Tractament perquè demostrin el seu compliment en matèria de protecció de dades.

ASPACE disposa d'un llistat actualitzat amb tots els Encarregats de Tractament on es relaciona:

- L'empresa responsable de l'Encarregat de Tractament
- L'activitat desenvolupada
- La vigència del contracte

Aquest llistat constitueix el Registre 10 d'encarregats de tractament, descrit a l'Annex 1.

9.6 Tercers sense accés a la informació

Els tercers que no tinguin accés a les dades han de signar un compromís de confidencialitat (del qual se'n recull un model a l'Annex 15) per tal de guardar secret en cas que es doni una situació en què s'accedeixi a alguna dada d'ASPACE.

10 Annexes

A continuació es llisten els annexes al present document. Tots ells són documents separats de l'actual per tal d'afavorir-ne el manteniment i detallar els aspectes més tècnics, però queden inclosos a tots els efectes dins de la política de seguretat d'Aspace.

Nom annex	Descripció breu
Annex 0 – Relació de fitxers declarats a l'AEPD	Detalla les principals característiques dels fitxers amb DCP declarats a l'AEPD per ASPACE.
Annex 1 - Registres	Descriu els formats i ubicació de cada un dels registres vinculats a la present política.
Annex 2 – Procediment d'encriptació segura d'arxius	Detalla el procediment per a encriptar fitxers informàtics, per a aquells casos en què cal transmetre'ls per mitjans no segurs.
Annex 3 – GPOs	Inclou les polítiques definides a nivell de la xarxa informàtica.
Annex 4 – Models d'autoritzacions	Conjunt de documents model (plantilles) d'autoritzacions d'acord amb la LOPD.
Annex 5 – Drets ARCO	Descriu els procediments interns de compliment dels drets ARCO. Inclou altres documents model (plantilles)
Annex 6 – Política d'identificació d'equips	Detalla l'estàndard de nomenclatura dels diferents equips i dispositius informàtics.
Annex 7 – Obsolescència de la informació	Descriu el temps que ha de transcórrer abans que es pugui esborrar un determinat tipus d'informació.
Annex 8 – Parametrització anti-virus	Detalla els paràmetres de configuració de l'antivirus corporatiu.
Annex 9 – Destrucció i esborrat	Descriu els procediments a seguir per a eliminar la informació que ja no és útil de forma segura.
Annex 10 – Perfils d'usuari	Detalla els diferents perfils de seguretat definits a nivell dels sistemes d'informació.
Annex 11 – Model tecnològic del lloc de treball	Descripció dels tipus de llocs de treball i dels elements de Hardware i Software que els composen.
Annex 12 – Responsabilitats d'implementació	Detall de les persones i departaments responsables d'implementar els punts que es descriuen a la present política.
Annex 13 – Clàusules encarregats de tractament	Model de les clàusules a incloure en els contractes d'encarregats de tractament.
Annex 14 – Gestió d'incidències de seguretat	Detalla els procediments a seguir per a la gestió i documentació de les incidències de seguretat.

Nom annex	Descripció breu
Annex 15. Model de compromís de confidencialitat	Model per a signar per part d'una empresa tercera que no tingui accés a la informació
Annex 16. Proves semestrals de recuperació	Procediment que descriu les diferents proves a realitzar i el model dels resultats.
Annex 17. Procediment registre d'entrades i sortides	Procediment que descriu la manera d'omplir el registre d'entrades i sortides per part dels diferents centres.
Annex 18. Desenvolupament d'aplicacions	Detalla els diferents entorns així com les bones pràctiques de programació.
Annex 19. Pautes d'ús del mòbil personal	Detalla en quins casos excepcionals es permet l'ús del mòbil personal a la feina, i quines pautes s'han de seguir.
Annex 20. Procediment d'arxiu físic	Procediment que descriu els processos lligats a qualsevol arxiu físic, i en concret la creació, el manteniment i l'el·liminació de l'arxiu.
Annex 21. Procediment per a sortides de lleure i respir	Procediment que descriu les mesures de seguretat a aplicar amb els dispositius i la informació que es fa servir en les sortides de lleure i respir.
Annex 22. Procediment de revisió de contractacions	Procediment que especifica que tots els nous contractes amb proveïdors hagin de revisar-se de cara al compliment de la LOPD.