FUNCIONS I OBLIGACIONS DELS EMPLEATS/DES

Entitat / Responsable del tractament:	Associació de Famílies d'Alumnes Escola Alba	G25053794
Responsable de protecció de dades i de seguretat informàtica:	Esther Pueyo Novau	ampaescolaalba@gmail.com

1. INTRODUCCIÓ

ASSOCIACIÓ AMPA ESCOLA ALBA, és una entitat compromesa amb la seguretat en la custòdia i tractament de la informació segons el que s'estableix en el Reglament General de Protecció de Dades (RGPD), d'aplicació directa a tots els Estats membres a partir del 25 de maig de 2018, que actualment es completa amb la normativa estatal espanyola, d'entrada en vigor el 7 de desembre de 2018, Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals (LOPDGDD).

Per això, totes les persones que treballen o col·laboren amb l'ENTITAT, adquireixen el compromís de complir les normatives vigents.

Les mesures i recomanacions que apareixen a continuació han de ser aplicades al tractament de la informació en general i, amb especial atenció, a les dades de caràcter personal en compliment de les normatives vigents.

Tot el personal que accedeixi informació de l'ENTITAT està obligat a conèixer i observar les mesures, normes, protocols, regles i estàndards que afecten les funcions que desenvolupa. Cada EMPLEAT/DA es responsabilitza del lloc de treball que té assignat i ha de complir amb els procediments interns de l'ENTITAT pel que fa a la protecció de dades personals.

S'estableixen les següents clàusules **d'obligat coneixement i compliment per TOTS els EMPLEATS/DES.**

2. CLÀUSULES

Clàusula Primera.- Àmbit d'aplicació del Document de Seguretat.

L'ENTITAT, com a Responsable dels tractaments de dades, declara disposar del Document de Seguretat que recull les mesures d'índole tècnica i organitzativa adaptades a les normatives de seguretat vigents, que són d'obligat compliment per al personal amb accés a dades de caràcter personal als sistemes d'informació i/o als recintes on se situen.

Clàusula Segona.- Tractament de dades personals.

S'entendrà com a tractament "tot conjunt organitzatiu de dades de caràcter personal, que permeti l'accés a les dades d'acord amb determinats criteris, qualsevol sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés". L'ENTITAT declara mantenir tractaments per al correcte desenvolupament de la seva activitat professional.

Clàusula Tercera.- Drets que emparen als afectats.

S'entendrà com a Afectat o Interessat a la "persona física titular de les dades que siguin objecte de tractament". Els drets d'accés, rectificació, supressió, portabilitat de les seves dades i a la limitació o oposició del seu tractament, així com no ser objecte de decisions individuals automatitzades formen part del contingut essencial del dret fonamental a la protecció de dades. Es tracta de drets l'exercici

dels quals és personalíssim, de caràcter gratuït i subjecte a terminis. Mitjançant el seu exercici l'afectat pot exercir control sobre els tractaments efectivament realitzats per l'ENTITAT, per la qual cosa ha establert procediments per a la seva satisfacció.

Cal tenir present l'obligació de comunicar qualsevol coneixement de sol·licitud de l'exercici de drets, tan aviat com sigui conegut, al responsable de seguretat designat.

Clàusula Quarta.- Deure de secret.

Guardant secret respecte de totes les dades de caràcter personal contingudes als tractaments de dades amb els quals hagi de treballar o tenir accés, segons la categoria laboral, sigui durant o després de finalitzar la seva relació amb l'ENTITAT.

En cap cas podrà divulgar o comentar amb cap persona aliena a l'ENTITAT, la informació que coneix sobre l'organització, clients, usuaris, familiars o tercers amb qui col·labori l'entitat.

Clàusula Cinquena.- Funcions i finalitat del tractament de les dades.

L'EMPLEAT/DA es compromet a no utilitzar les dades ni la informació a la qual tingui accés, per a finalitats diferents de les assignades, d'acord amb les funcions encomanades.

Clàusula Sisena.- Limitació al tractament.

Qualsevol tractament de dades destinat a altres finalitats no encomanades a l'EMPLEAT/DA es considerarà com no autoritzat per l'ENTITAT. No recopilarà dades de caràcter personal ni crearà fitxers que continguin dades de caràcter personal sense l'autorització expressa i explicita de l'ENTITAT. Únicament podrà realitzar processos de captació, tractament i sortida de dades, per a aquells tractaments en els quals figuri autoritzat, havent de regir-se per les normes establertes en el present document. **L'ús i tractament de les dades per a finalitats privades, amb o sense ànim de lucre, queda totalment prohibit.**

Clàusula Setena.- Seguretat de les dades.

L'EMPLEAT/A es compromet a vetllar per la seguretat de les dades amb les eines i controls implantats per l'ENTITAT, i en cap concepte permetrà que tercers no autoritzats puguin accedir a aquestes dades, sigui de forma informàtica o visual, o qualsevol altra forma que en el futur pugui aparèixer.

Clàusula Vuitena.- Responsable de protecció de dades i de seguretat informàtica.

Es designa un responsable de seguretat de protecció de dades i seguretat informàtica que s'encarregarà de coordinar i controlar les mesures definides en el Document de Seguretat, servint al mateix temps d'enllaç entre el/la empleat/a i l'ENTITAT, sense que això suposi en cap cas una delegació de la responsabilitat que correspon a aquesta última.

Clàusula Novena.- Notificació i gestió de violacions de seguretat, incidències.

En el moment de tenir coneixement d'una violació de seguretat o incidència s'haurà de comunicar **immediatament** al Responsable de Seguretat de l'ENTITAT.

S'entendrà com a violació de seguretat o incidència "qualsevol anomalia que afecti o pogués afectar la seguretat de les dades".

El coneixement i la no notificació d'una incidència per part d'un empleat o empleada seran considerats com una falta contra la seguretat del tractament.

Clàusula Desena.- Salvaguarda i protecció de les contrasenyes personals.

L'assignació i la distribució inicial de les contrasenyes estan a càrrec del departament de suport informàtic de l'ENTITAT. Una vegada hagin estat comunicades als usuaris, aquests hauran de modificar la seva clau i guardar secret respecte de les claus d'accés i qualsevol altra mesura de seguretat que sigui atorgada. Cada EMPLEAT/DA serà responsable de la confidencialitat de la seva contrasenya i, en cas de coneixement fortuït o fraudulentament per persones no autoritzades, haurà de registrar-se com a incidència i procedir immediatament al canvi d'aquesta.

La periodicitat màxima de les contrasenyes es fixa en anual. El format i longitud de les mateixes vindrà establert i s'haurà de respectar, sense disposar l'usuari d'autorització per a suprimir-les.

Clàusula Onzena.- Gestió de suports.

L'usuari tractarà les dades que li siguin subministrades i contingudes en els tractaments titularitat de l'ENTITAT als seus propis locals i sistemes d'informació.

Els suports, siguin documents o automatitzats (pen drive, PC, Tablet, dispositius portàtils, PDA, etc.), que continguin dades, hauran d'estar clarament identificats, indicant de quin arxiu es tracta, quin tipus de dades contenen, l'usuari al càrrec i la data de la seva creació.

Clàusula Dotzena.- Accés a suports.

Els suports on hi hagi dades personals hauran de ser emmagatzemats en llocs protegits on persones que no tinguin autorització no hi tinguin accés, i disposaran de controls per a evitar l'accés indegut. Es preservarà que la informació que mostrin no pugui ser visible per a persones no autoritzades.

Quan l'usuari a càrrec del suport deixi d'utilitzar-lo, bé temporalment o bé en finalitzar el seu treball, el deixarà en un estat que impedeixi la visualització de les dades protegides.

Per als suports automatitzats, com a equips de treball, això podrà realitzar-se a través d'un protector de pantalla que impedeixi la visualització de les dades. La volta al treball implicarà la desactivació de la pantalla protectora amb la introducció de la contrasenya corresponent.

Per als suports documentals implicarà l'arxiu dels mateixos en dispositius que obstaculitzin l'obertura per tercers no autoritzats.

Clàusula Tretzena.- Generació de còpies i destrucció de suports.

L'usuari no té autorització per a crear còpies de documents, de bases de dades, de fitxers o informació, als quals tingui accés per la seva activitat laboral a través de mitjans informàtics, documentals, visuals i/o qualsevol altre mitjà. Serà l'ENTITAT, a través del responsable de seguretat o responsable de seguretat informàtica designat, qui autoritzarà la realització d'aquestes còpies, també s'ocuparà d'establir els procediments de seguretat i recuperació de les dades necessàries.

La destrucció de dades en suports documentals es realitzarà adoptant un mecanisme que garanteixi la no recuperació posterior (per exemple, destructora homologada) i haurà de ser prèviament autoritzada per l'ENTITAT a través del responsable de seguretat o responsable de seguretat informàtica designat.

Després de finalitzar qualsevol tractament de dades o bé després de la seva vinculació laboral amb l'ENTITAT, l'EMPLEAT/DA haurà de retornar qualsevol suport que contingui dades de propietat de l'ENTITAT, preservant la seguretat de la informació durant el seu trasllat o transmissió. Amb posterioritat procedirà a l'esborrat complet de les dades i de les còpies que poguessin ser

emmagatzemades als sistemes propietat de l'usuari (dispositius mòbils, compte de correu electrònic personal, o uns altres).

Clàusula Catorzena.- Sortida de dades i xifrat.

Quan la sortida de dades de l'arxiu es realitzi per mitjà de correu electrònic, els enviaments es realitzaran sempre i únicament des d'una adreça de correu controlada per l'ENTITAT, deixant constància d'aquest enviament al directori històric d'aquesta adreça de correu o en algun altre sistema de registre de sortida que permeti conèixer en qualsevol moment els enviaments realitzats, a qui van dirigits i la informació enviada.

Quan les dades del tractament que hagin de ser enviades siguin de **dades sensibles s'enviaran xifrades, de manera que només pugui ser llegides i interpretades pel destinatari, al qual facilitarem la clau per desxifrar el document mitjançant un altre sistema d'enviament.** L'EMPLEAT/DA disposarà de mecanisme o eina que permeti el xifrat d'arxius de forma senzilla subministrada pel responsable de seguretat de l'ENTITAT. Qualsevol dubte que li pugui sorgir a l'EMPLEAT/DA o anomalia que es produeixi en els mecanismes de xifrat i que impedeixi el seu correcte ús haurà de ser considerat una incidència i notificar-la seguint el procediment establert.

L'EMPLEAT/DA comunicarà i sol·licitarà autorització al responsable de Seguretat, per a la sortida de suports i qualsevol transferència de dades que necessiti realitzar.

Clàusula Quinzena.- Registre dels accessos.

L'ENTITAT podrà monitorar l'activitat de l'EMPLEAT/DA mitjançant de mecanismes de registre d'accessos al tractament, que continguessin dades de caràcter personal propietat de l'ENTITAT Qualsevol intent de desactivació dels mecanismes de registre per part de l'EMPLEAT/DA es considerarà una falta contra la seguretat del tractament.

Clàusula Setzena.- Correu Electrònic.

L'ENTITAT es reserva el dret de revisar, sense previ avís, els missatges de correu electrònic dels usuaris de la xarxa corporativa, amb la finalitat de comprovar el compliment d'aquestes normes i prevenir activitats que puguin afectar l'ENTITAT com a responsable civil subsidiari.

L'EMPLEAT/DA, per a donar compliment del deure d'informació, utilitzarà la signatura i clàusula de correu electrònic, facilitada per l'ENTITAT, que incorporarà la informació als peus dels correus, siguin nous, respostes o reexpedicions.

Clàusula Dissetena.- Accés a Internet/Intranet.

L'ús del sistema informàtic de l'ENTITAT per a accedir a xarxes públiques com Internet, es limita als temes directament relacionats amb l'activitat de l'ENTITAT i les funcions inherents al lloc de treball de l'EMPLEAT/DA.

L'accés a debats en temps real (xats / IRC) és especialment perillós, ja que facilita la instal·lació d'utilitats que permetin accessos no autoritzats al sistema, per la qual cosa queda estrictament prohibit.

L'accés a pàgines web (www), grups de notícies (newsgroups) i d'altres fonts d'informació com FTP, Intranet o unes altres, es limita a aquelles que continguin informació relacionada amb l'activitat de l'ENTITAT o amb les funcions inherents al lloc de treball de l'EMPLEAT/DA. L'ENTITAT es reserva el dret de monitorar i comprovar, de forma aleatòria i sense previ avís, qualsevol sessió d'accés a Internet iniciada per un usuari de la xarxa corporativa.

Qualsevol fitxer introduït en la xarxa corporativa o terminal utilitzat per l'EMPLEAT/DA des d'Internet ha de complir els requeriments establerts per aquesta normativa i, especialment, les relatives a la propietat intel·lectual i el control de virus i altres amenaces.

Clàusula Divuitena.- Xarxes socials corporatives - Procediment de sol·licitud creació.

Si no es disposa d'AUTORITZACIÓ, NO es pot crear cap compte corporatiu, a cap xarxa social.

L'EMPLEAT/DA que estigui interessat/da en crear un nou compte corporatiu, a qualsevol xarxa social, sol·licitarà autorització al responsable de l'ENTITAT, comunicar-li la iniciativa i detallar els seus objectius i les xarxes socials seleccionades.

L'ENTITAT analitzarà la iniciativa i si és aprovada, donarà d'alta el nou compte corporatiu a la xarxa social seleccionada. L'ENTITAT s'encarregarà de configurar el nou compte de la xarxa social (fons, avatars, nomenclatures,...) i a facilitar a la persona sol·licitant les eines de gestió del compte sol·licitat.

Clàusula Dinovena.- WhatsApp

En representació de l'ENTITAT, no es pot administrar cap grup de WhatsApp, ni formar-ne part, sense AUTORITZACIÓ.

Si es determina l'ús de la plataforma WhatsApp com a mitjà de comunicació, s'han de llegir i respectar les condicions d'ús de la plataforma.

Per realitzar enviaments d'informació, és necessari disposar del consentiment explícit del destinatari/interessat i complir amb el deure d'informar.

Clàusula Vintena.- Prohibicions expresses.

Estan expressament prohibides les següents activitats:

- **Utilitzar i tractar les dades per a finalitats privades, amb o sense ànim de lucre.**
- **La no notificació d'una incidència de la qual es tingui coneixement.**
- **Intentar augmentar el nivell de privilegis d'un usuari/a en el sistema.**
- **Utilitzar el sistema per a intentar accedir a àrees restringides dels sistemes informàtics de l'ENTITAT o de tercers.**
- **Instal·lar còpies il·legals de qualsevol programa, inclosos els estandarditzats.**
- **Intentar desxifrar les claus, contrasenyes, sistemes o algorismes de xifrat o qualsevol altre element de seguretat (control d'accessos, registres d'accessos, antivirus, actualitzacions automàtiques, etc.) implantat pel personal administrador de l'ENTITAT.**
- **Destruir, alterar, inutilitzar o de qualsevol forma danyar les dades, programes o documents tan automatitzats com en paper de l'entitat o tercers. (Això pot constituir un delicte de danys, previst en l'article 262,2 del Codi Penal).**

- **Introduir voluntàriament programes, virus, macros, miniaplicacions, controls Actius o qualsevol altre dispositiu lògic o seqüència de caràcters que causin o siguin susceptible de causar qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o tercers.**
- **Introduir continguts obscens, immorals o ofensius, o uns altres que en general, manquen d'utilitat per als objectius de l'entitat en la xarxa corporativa d'aquesta, ja sigui a través del correu electrònic o altres mitjans.**
- **Utilitzar els recursos telemàtics de l'entitat, inclosa la xarxa d'Internet, per a activitats que no es trobin directament relacionades amb les funcions inherents al lloc de treball de l'usuari.**
- **Enviar missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitaris sense el consentiment del destinatari.**
- **Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris. (Aquesta activitat pot constituir un delicte d'intercepció de les comunicacions, previst en l'article 197 del Codi Penal).**
- **Compartir o facilitar les identificacions d'usuari i les claus d'accés facilitades per l'ENTITAT a una altra persona física o jurídica, inclòs el personal de la mateixa entitat. En cas d'incompliment d'aquesta prohibició, l'EMPLEAT/DA és l'únic responsable de les actuacions realitzades per la persona física o jurídica que utilitzi de forma no autoritzada la identificació de l'usuari.**
- **Dins de l'horari laboral no està permès l'ús dels dispositius mòbils. La utilització dels mòbils particulars durant la jornada laboral poden ocasionar problemàtiques durant la prestació dels serveis, sense oblidar el risc que això suposa per a la mateixa seguretat de l'empleat/da i dels usuaris/es. Per tant, heu d'entrar a treballar sense el telèfon mòbil o l'heu de deixar al bolso, bossa o motxilla, en cap cas portar-lo al damunt encès. Podeu facilitar el telèfon fix de l'entitat, a qui cregueu necessari, perquè us puguin localitzar en cas d'urgència.**
- **Queda prohibit de realitzar fotos o vídeos a l'interior de les instal·lacions del centre de treball, amb qualsevol mena de dispositiu (telèfon mòbil, càmera fotogràfica o de vídeo, etc,...). Queda prohibit captar imatges de persones, de documents, d'espais del centre,**

de bases de dades, de protocols i formes d'organització i actuacions internes com ara: organització de tasques per torn, fulls d'anotacions de personal, registres, horaris o qualsevol altre document.

3. MESURES DE SEGURETAT I BONES PRÀCTIQUES.

La confidencialitat de la informació s'aconsegueix també a través de la cura de l'entorn de treball, evitant que la mateixa pugui ser de fàcil accés per qualsevol. Per això s'estableixen diverses actuacions d'obligat compliment.

Considerar la informació com un actiu fonamental l'ENTITAT complint les següents mesures:

- Pel que fa als **ordinadors portàtils i resta de dispositius d'emmagatzematge mòbils (telèfons mòbils, memòries USB, tablets, etc.)**, s'ha de complir:
    1. Mantenir-sempre controlats, (no deixar en llocs públics, taxis, etc.) per evitar la seva sostracció.
    2. Reduir i/o eliminar la informació que no hagi de ser utilitzada.

- En cas de **pèrdua o robatori d'un dispositiu d'emmagatzematge mòbil** (portàtil, telèfon, memòria USB, tablets, etc.) s'ha de **notificar immediatament com a incidència de seguretat.**

- És molt important que **no s'emmagatzemin ni tractin dades de caràcter personal al disc dur** de l'equip a causa de l'alt risc de pèrdua de dades i d'accessos no autoritzats. Aquestes accions s'han de fer en els entorns proveïts a aquest efecte (carpetes dels servidors, aplicacions, etc.) protegits mitjançant identificadors d'usuari amb els permisos corresponents..

- Respecte al **correu electrònic i Internet**, s'ha de prestar atenció a l'enviament de dades de caràcter personal per mitjà del correu electrònic, tant en el cos del missatge com annexos i, si es realitza, tractar aquests missatges i annexos com a temporals i esborrar-los quan deixin de ser necessaris. **El correu electrònic no és un gestor documental**, els fitxers enviats o rebuts han d'estar emmagatzemats en els sistemes i carpetes corresponents protegits per les credencials d'usuari corresponents.

- No s'han d'obrir correus procedents d'adreces desconegudes o que no estiguin relacionats amb motius de treball i ofereixin les suficients garanties, per evitar l'entrada de virus, troians o codi maliciós.

- No obrir adjunts a correus o prémer en enllaços, llevat que siguin coneguts i l'origen de confiança, tant del correu com de l'enllaç.

- No es podrà utilitzar el correu per a finalitats diferents a les corporatives.

- No realitzar reenviament massiu de correus i sempre que es faci, utilitzar CCO (enviar amb còpia oculta), quan s'envia a diferents destinataris, per tal d'ocultar la visualització de les diferents adreces de correu.

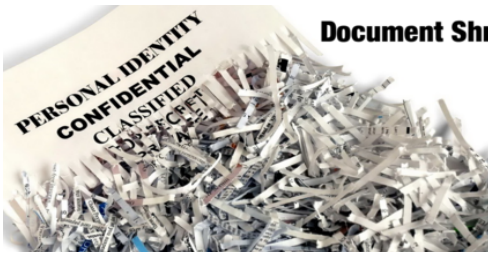
- **Taules netes:** cada usuari, cada vegada que s'absenti de la seva taula de treball o bé quan acabi la seva jornada laboral, haurà de retirar tota aquella informació que contingui informació que pogués ser de caràcter confidencial.

- **Utilització de fotocopiadores, escàners i impressores**: En utilitzar impressores o fotocopiadores, assegureu-vos de recollir els originals al finalitzar i que no quedin documents amb dades sensibles a la safata de sortida. Si les impressores són compartides amb altres usuaris sense accés a les dades que estan sent impresos, s'hauran de retirar els documents conforme vagin sent impresos.

  De forma anàloga, en utilitzar els escàners, assegureu-vos de recollir els documents originals i, si la carpeta de destinació es comparteix amb usuaris sense accés a aquestes dades personals, eliminar l'arxiu el més aviat possible d'aquesta carpeta i traslladar-lo a una altra carpeta amb un nivell de seguretat d'acord a les dades que contenen.

- **Utilització de fax:** quan es vagi a enviar un fax sempre s'ha d'avisar al destinatari perquè estigui pendent de la recollida de la informació. Quan s'espera rebre informació amb dades personals per aquest mitjà és important demanar a la persona que l'envia que ens avisi per estar atents a l'arribada de la documentació.

- **Eliminació de documents:** utilitzar els dispositius destinats a aquest efecte per eliminar el material corresponent, és a dir, dipositar-la en els contenidors destinats a aquest efecte o en les destructores de paper. Si es tira documentació a les papereres, aquesta haurà de trencar-se prèviament de manera que la informació que conté quedi inintel·ligible.



- **Distribució de la documentació:** adoptar mesures cautelars que evitin accessos no autoritzats. Es poden produir diferents situacions en el moviment dels fitxers en paper:

  - Enviaments fora del centre de treball: sempre ha de sortir en sobre tancat o dispositiu de seguretat similar que eviti accessos de tercers, de manera que no es pugui realitzar consulta, còpia o reproducció de la mateixa. També pot utilitzar-se un servei de valisa interna.

- Enviaments dins del centre de treball: per a enviaments dins el mateix edifici on es troba el nostre lloc de treball, s'han d'utilitzar els mitjans implantats a la l'ENTITAT de manera que s'evitin accessos no desitjats.

    - Comprovar que les persones a les que es lliura la documentació original o una còpia de la mateixa l'han rebut.

    - No retirar de les dependències suports o fitxers no automatitzats sense la deguda autorització.

4. CONSEQÜÈNCIES DE L'INCOMPLIMENT

L'ENTITAT o RESPONSABLE informa a l'EMPLEAT/DA, com a personal amb accés als sistemes i als seus arxius, de les conseqüències i les responsabilitats en què puguin incórrer en cas d'incompliment de la normativa de seguretat, que podria derivar en sancions.

L'incompliment per part de l'EMPLEAT/DA de les obligacions establertes en el manual de normes de seguretat i la normativa interna relacionada amb la protecció de dades personals, així com la comissió de les infraccions tipificades en les normatives vigents en Protecció de Dades, podrà ser sancionat d'acord amb la legislació del règim disciplinari aplicable.

L'EMPLEAT/DA assumeix qualsevol responsabilitat legal que es derivi de l'incompliment per part dels compromisos continguts en aquest document i tots els seus annexos, i pot derivar en una reclamació de danys i perjudicis.

Serà el Responsable, l'ENTITAT, ja sigui per si mateix o per mitjà de tercers degudament autoritzats i designats, qui determinarà la gravetat (lleu, greu, molt greu) de les faltes i les conseqüències, posant-ho en coneixement de l'EMPLEAT/DA.

En cas de produir-se una incidència, serà el responsable de seguretat designat per l'ENTITAT, qui s'encarregarà de gestionar-la establint un registre en què es faci constar el tipus d'incidència, el moment en què es va produir, o, si s'escau va ser detectada, la persona que va fer la notificació, a qui se li va comunicar, els efectes que es puguin derivar de la mateixa i les mesures correctores aplicables.

En/Na_____

amb D.N.I.:_____, EMPLEAT/DA, he rebut i llegit el document "**FUNCIONS I OBLIGACIONS DELS EMPLEATS/DES**" que conté la informació per a tractar les dades personals segons l'establert al Reglament General de Protecció de Dades UE 2016/679 (RGPD) i Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals (LOPDGDD).

A _____, ___ de _____ del 20__

Signat: