I.N.E.F.C.

inefc Institut Nacional d'Educació Física de Catalunya

R/N: INEFC/CP00034 INEFC-2024-3

Acord d'encàrrec de tractament de dades de caràcter personal entre l'Institut Nacional d'Educació Física de Catalunya i UNIVERSITAS XXI, Soluciones y Tecnología para la Universidad, S.A., vinculat al contracte del servei de manteniment del sistema integrat de gestió acadèmica, UNIVERSITAS XXI, per als centres de Barcelona i de Lleida de l'INEFC, expedient INEFC-2024-3.

REUNITS

D'una part, el senyor Eduard Inglés Yuba, director de l'Institut Nacional d'Educació Física de Catalunya, organisme autònom del Departament de la Presidència de la Generalitat de Catalunya, NIF Q0840010C, en virtut de la renovació del nomenament de data 11 de juny de 2024 (Decret 105/2024, d'11 de juny; DOGC núm. 9182, de 12.6.2024) i de les facultats que li confereix l'article 9.2 c), de la Llei 11/1984, de 5 de març, de creació de l'organisme autònom Institut Nacional d'Educació Física de Catalunya (en endavant INEFC);

I d'altra part, la senyora Raquel Bermejo Martínez, en nom i representació de l'empresa UNIVERSITAS XXI, Soluciones y Tecnología para la Universidad, S.A. (en endavant UXXI, SA), NIF núm. A80897770, amb domicili social al carrer Arequipa, núm. 1, de Madrid (28043), segons escriptura de poder mercantil, protocol 2776, autoritzada pel notari de l'Il·lustre Col·legi Notarial de Madrid, senyor Antonio Álvarez Pérez, en data 21 d'octubre de 2019.

Ambdues parts, en l'exercici de les funcions que els estan legalment assignades, reconeixent-se recíprocament la capacitat legal necessària per obligar-se, de comú acord,

MANIFESTEN

I. Que ambdues parts han signat un contracte que té per objecte el servei de manteniment del sistema integrat de gestió acadèmica, UNIVERSITAS XXI, pels dos centres de l'INEFC, expedient INEFC-2024-3.

II. La necessitat de signar un acord d'encàrrec de tractament de dades de caràcter personal en relació a l'esmentat contracte, en els termes que estableix els articles 28 del RGPD i 33 de la LOPDGDD.

Generalitat de Catalunya

inefc Institut Nacional d'Educació Física de Catalunya

CLÀUSULES

Primera. Objecte de l'encàrrec de tractament

Mitjançant aquest acord d'encàrrec s'habilita a UXXI, SA, en qualitat d'encarregat del tractament (en endavant, l'encarregat), per tractar per compte de l'INEFC , responsable del tractament (en endavant, el responsable), les dades de caràcter personal necessàries per prestar el servei de manteniment del sistema integrat de gestió acadèmica, UNIVERSITAS XXI, per als centres de Barcelona i de Lleida de l'INEFC, expedient INEFC-2024-3.

El tractament consistirà en:

El control i el seguiment dels expedients acadèmics de l'alumnat i del professorat; i assegurar la comunicació institucional acadèmica a tot l'alumnat i el professorat incloent-hi els projectes de recerca propis dels centres de l'INEFC. Concretament: gestionar la preinscripció i la matriculació de l'alumnat de grau, màster, doctorat i de l'Escola de Tècnics Esportius i de formació continuada i, en general, de tota l'activitat acadèmica de l'INEFC, incloent-hi les activitats derivades del funcionament dels diversos òrgans col·legiats propis de l'estructura acadèmica de l'INEFC i de les seves funcions quant a les comunicacions i activitats. Fer el seguiment del progrés acadèmic de l'alumnat i del professorat, gestionar l'activitat i el desenvolupament acadèmics, en general. Tractament estadístic de les dades.

Concreció dels tractaments a realitzar:

☐ Recollida	☐ Registre
☑ Estructuració	☑ Modificació
☑ Conservació	☐ Extracció
☑ Consulta	☑ Comunicació per transmissió
☐ Difusió	☐ Interconnexió
☐ Acarament	☐ Limitació
☑ Supressió	☐ Destrucció
☐ Comunicació	☑ Altres: Accés a les dades i Elaboració de còpies

Segona. Identificació de la informació afectada

Per executar les prestacions derivades del compliment de l'objecte d'aquest encàrrec, el responsable, posa a disposició de l'encarregat, el tractament de dades "Gestió d'expedients acadèmics de l'INEFC". La informació completa d'aquest tractament es pot trobar en el

Registre d'activitats de tractament de l'INEFC i a l'espai de "protecció de dades" publicat al web de l'INEFC, i és la que s'indica a continuació:

- Responsable del tractament: gerència de l'INEFC, Av. de l'Estadi 12-22, 08038 Barcelona. Correu electrònic; inefc.pd@gencat.cat

- Delegat de protecció de dades del departament de la Presidència: Sant Honorat 2-4, 08002 Barcelona. Correu electrònic dpd.presidencia@gencat.cat

- Finalitat del tractament**:** control i seguiment dels expedients acadèmics La finalitat del tractament és el control i el seguiment dels expedients acadèmics de l'alumnat i del professorat; assegurar la comunicació institucional acadèmica a tot l'alumnat i el professorat incloent-hi els projectes de recerca propis dels centres de l'INEFC. Concretament: gestionar la preinscripció i la matriculació de l'alumnat de grau, màster, doctorat i de l'Escola de Tècnics Esportius i de formació continuada i, en general, de tota l'activitat acadèmica de l'INEFC, incloent-hi les activitats derivades del funcionament dels diversos òrgans col·legiats propis de l'estructura acadèmica de l'INEFC i de les seves funcions quant a les comunicacions i activitats. Fer el seguiment del progrés acadèmic de l'alumnat i del professorat, gestionar l'activitat i el desenvolupament acadèmics. Tractament estadístic.

- Finalitat exclusiva de l'accés a dades personals per part de l'encarregat: La gestió de l'aplicació UNIVERSITAS XXI, propietat de l'empresa UXXI S.A., que permet la gestió de les dades de l'alumnat de l'INEFC contingudes en els seus expedients acadèmics, exclusivament per al desenvolupament de les tasques directament relacionades amb l'objecte del contracte.

- Categoria de persones interessades**:** personal administratiu, personal docent i investigador (PDI), alumnes de l'INEFC, així com els seus representants legals.

- Categoria de les dades personals:

  Dades de caràcter identificatiu: nom i cognoms, NIF o document identificatiu equivalent, Núm. d'afiliació a la Seguretat Social (NASS), targeta sanitària, adreça postal i electrònica, telèfon, signatura, imatge.

  Dades de característiques personals: sexe, dades familiars: identificatives de pares, mares, tutors, o persona representant, germans, data i lloc de naixement, nacionalitat, Títol de Família Nombrosa (TFN).

  Dades econòmiques i financeres: dades bancàries, assegurança escolar, acreditacions com a becari/ària, certificats mèdics i documents de minusvalidesa (certificacions de l'ICASS).

Dades acadèmiques i professionals:

- Alumnes: targeta de les Proves d'Accés a la Universitat (PAU), dades d'accés a la universitat, formació, títols, historial acadèmic, acreditacions com a esportistes d'elit o alt rendiment.
- Professorat: experiència professional, formació, títols, historial acadèmic, contractes i/o nomenaments, acreditacions (lector, col·laborador, agregat, etc.) davant de les agències nacionals (ANECA, AQU)

- Categories de persones destinatàries a les quals es poden comunicar les dades personals: a les universitats on està adscrit l'INEFC (UB i UdL), altres instituts d'educació física de l'Estat espanyol i a entitats públiques i privades (entitats bancàries gestores dels pagaments de matrícules, Piscines Bernat Picornell, AGAUR, AQU, INE i d'altres centres col·laboradors en la prestació de serveis acadèmics).

- Transferències internacionals de dades: es preveu la transferència amb l'empresa filial UNIVERSITAS XXI Soluciones y Tecnología para la Universidad Colombia SAS (subencarregada), que s'encarrega de la monitorització i gestió dels entorns gestionats per UNIVERSITAS XXI Soluciones y Tecnología para la Universidad, S.A. (encarregada), amb la que té firmat un contracte de confidencialitat i encarregat de tractament d'acord amb les clàusules tipus fixades per la decisió d'execució (UE) 2021/915 de la comissió de 4 de juny de 2021.

- Termini previst de supressió de les dades: indefinit.

- Descripció general de les mesures tècniques i organitzatives de seguretat: les adequades a un nivell de seguretat mitjà.

Tercera. Durada

La vigència d'aquest acord d'encàrrec de tractament queda vinculada a la vigència del contracte subscrit, expedient INEFC-2024-3.

Una vegada finalitzat aquest contracte, l'encarregat del tractament ha de retornar al responsable les dades personals i suprimir qualsevol còpia que estigui en el seu poder.

Quarta. Obligacions de l'encarregat del tractament

L'encarregat del tractament, i tot el seu personal s'obliguen a:

a) Utilitzar les dades personals objecte de tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest encàrrec. En cap cas pot utilitzar les dades per a finalitats pròpies.

b) Tractar les dades d'acord amb les instruccions del responsable del tractament.

Si l'encarregat del tractament considera que alguna de les instruccions infringeix el RGPD o qualsevol altra disposició en matèria de protecció de dades de la Unió o dels estats membres, l'encarregat n'ha d'informar immediatament el responsable.

c) Portar, per escrit, en els casos previstos per la normativa en matèria de protecció de dades, un registre de totes les categories d'activitats de tractament efectuades per compte del responsable, que contingui:

1. El nom i les dades de contacte de l'encarregat i del responsable per compte del qual actua l'encarregat i, del delegat de protecció de dades.
2. Les categories de tractaments efectuats per compte del responsable.
3. Si escau, les transferències de dades personals a un tercer país o organització internacional, inclosa la identificació d'aquest país o aquesta organització internacional, i en el cas de les transferències indicades a l'article 49, apartat 1, paràgraf segon del RGPD, la documentació de garanties adequades.
4. Una descripció general de les mesures tècniques i organitzatives de seguretat relatives a:

- La pseudonimització i el xifrat de dades personals.
- La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.
- La capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida, en cas d'incident físic o tècnic.
- El procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives que garanteix la seguretat del tractament.

d) No comunicar les dades a terceres persones, tret que tingui l'autorització expressa del responsable del tractament, en els supòsits legalment admissibles.

L'encarregat pot comunicar les dades a altres encarregats del tractament del mateix responsable, d'acord amb les instruccions del responsable. En aquest cas, el responsable ha d'identificar, prèviament i per escrit, l'entitat a la qual s'han de comunicar les dades, les dades a comunicar i les mesures de seguretat que cal aplicar per procedir a la comunicació.

Si l'encarregat ha de transferir dades personals a un tercer país o a una organització internacional, en virtut del dret de la Unió o dels estats membres que li sigui aplicable,

ha d'informar el responsable d'aquesta exigència legal de manera prèvia, tret que aquest dret ho prohibeixi per raons importants d'interès públic.

e) S'autoritza l'encarregat a subcontractar amb **Arsys Internet S.L.U.,** les prestacions que comporten els tractaments següents: allotjament de les dades i a subencarregar amb la filial **UNIVERSITAS XXI Soluciones y Tecnología para la Universidad Colombia S.A.S**, les prestacions que comporten els tractaments següents: monitorització i gestió dels entorns gestionats, amb les que manté firmat un contracte de confidencialitat i encarregat de tractament.

   Per subcontractar amb altres empreses, l'encarregat ha de comunicar aquest fet per escrit al responsable i identificar de forma clara i inequívoca l'empresa subcontractista i les seves dades de contacte. La subcontractació es pot dur a terme si el responsable no hi manifesta oposició en el termini de 20 dies.

   El subcontractista, que també té la condició d'encarregat del tractament, està obligat igualment a complir les obligacions que aquest document estableix per a l'encarregat del tractament i les instruccions que dicti el responsable. Correspon a l'encarregat inicial regular la nova relació, de manera que el nou encarregat quedi subjecte a les mateixes condicions (instruccions, obligacions, mesures de seguretat…) i amb els mateixos requisits formals que ell, pel que fa al tractament adequat de les dades personals i a la garantia dels drets de les persones afectades. Si el subencarregat ho incompleix, l'encarregat inicial continua sent plenament responsable davant el responsable pel que fa al compliment de les obligacions.

f) Mantenir el deure de secret respecte de les dades de caràcter personal a les quals hagi tingut accés en virtut del present encàrrec. Aquestes obligacions subsistiran, fins i tot posteriorment a l'extinció de la relació entre UXXI, SA i l'INEFC.

g) Garantir que les persones autoritzades per tractar dades personals es comprometen, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les quals cal informar-los convenientment.

h) Mantenir a disposició del responsable la documentació que acredita que es compleix l'obligació que estableix l'apartat anterior.

i) Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per tractar dades personals.

j) Assistir el responsable del tractament en la resposta a l'exercici dels drets següents:

   1. Accés, rectificació, supressió i oposició.
   2. Limitació del tractament.
   3. A no ser objecte de decisions individualitzades automatitzades (inclosa l'elaboració de perfils).

Quan les persones afectades exerceixin els drets d'accés, rectificació, supressió i oposició, limitació del tractament, portabilitat de dades i a no ser objecte de decisions individualitzades automatitzades, davant l'encarregat, aquest ho ha de comunicar per correu electrònic a l'adreça inefc.pd@gencat.cat. La comunicació s'ha de fer de forma immediata i en cap cas més enllà de l'endemà del dia laborable en què s'ha rebut la sol·licitud, juntament, si escau, amb altres informacions que puguin ser rellevants per resoldre la sol·licitud.

j) Dret d'informació

Correspon al responsable facilitar el dret d'informació en el moment de recollir les dades.

k) Notificació de violacions de la seguretat de les dades

L'encarregat del tractament ha d'informar el responsable del tractament, sense dilació indeguda i en qualsevol cas abans de 48 hores, de les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per documentar i comunicar la incidència, per correu electrònic a l'adreça inefc.pd@gencat.cat.

La notificació no és necessària quan sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques.

Si se'n disposa, cal facilitar, com a mínim, la informació següent:

1. Descripció de la naturalesa de la violació de la seguretat de les dades personals, incloses, quan sigui possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.
2. Nom i dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual es pugui obtenir més informació.
3. Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
4. Descripció de les mesures adoptades o proposades per posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

Si no és possible facilitar la informació simultàniament, i en la mesura en què no ho sigui, la informació s'ha de facilitar de manera gradual sense dilació indeguda.

Correspon a l'encarregat del tractament comunicar en el menor temps possible als interessats les violacions de la seguretat de les dades, quan sigui probable que la violació suposi un alt risc per als drets i les llibertats de les persones físiques.

La comunicació s'ha de fer en un llenguatge clar i senzill i, com a mínim, cal:

a) Explicar la naturalesa de la violació de dades.

b) Indicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en què es pugui obtenir més informació.

c) Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.

d) Descriure les mesures adoptades o proposades pel responsable del tractament per posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

l) Donar suport al responsable del tractament a l'hora de fer les avaluacions d'impacte relatives a la protecció de dades, quan escaigui.

m) Donar suport al responsable del tractament a l'hora de fer les consultes prèvies a l'autoritat de control, quan escaigui.

n) Posar a disposició del responsable tota la informació necessària per demostrar que compleix les seves obligacions, així com per realitzar les auditories o les inspeccions que efectuïn el responsable o un altre auditor autoritzat per ell.

o) Implantar les mesures de seguretat incloses a l'annex 1 d'aquest acord, d'acord amb l'avaluació de riscos realitzada.

p) Designar un delegat de protecció de dades, en els casos previstos per la normativa en matèria de protecció de dades, i comunicar-ne la identitat i les dades de contacte al responsable.

q) Destinació de les dades

Retornar a l'INEFC, responsable del tractament, les dades de caràcter personal i, si escau, els suports on constin, una vegada complerta la prestació i finalitzada la vigència del contracte formalitzat entre les parts.

La devolució ha de comportar l'esborrat total de les dades existents en els equips informàtics utilitzats per UXXI, SA, encarregat del tractament.

No obstant això, l'encarregat pot conservar-ne una còpia, amb les dades degudament bloquejades, mentre es puguin derivar responsabilitats de l'execució de la prestació.

r) El contractista s'ha de sotmetre a la normativa nacional i de la Unió Europea en matèria de protecció de dades. Aquesta obligació té la condició d'obligació contractual essencial.

s) Quan l'execució del contracte impliqui la utilització de servidors per part del contractista, l'empresa adjudicatària ha de presentar, abans de formalitzar el contracte, i quan es produeixi qualsevol canvi durant l'execució del contracte, una declaració sobre el lloc on estaran ubicats els servidors i des d'on es prestaran els serveis associats a aquests.

t) Els licitadors han d'indicar a la seva oferta si tenen previst subcontractar els servidors o serveis associats a aquests i, en cas afirmatiu, el nom o el perfil empresarial dels subcontractistes, definit per referència a les condicions de solvència professional o tècnica.

Cinquena. Obligacions del responsable del tractament

Correspon al responsable del tractament:

a) Lliurar a l'encarregat les dades a les quals es refereix la clàusula 2 d'aquest document.

b) Fer una avaluació de l'impacte en la protecció de dades personals de les operacions de tractament que ha d'efectuar l'encarregat si fos preceptiu.

c) Fer les consultes prèvies a l'Autoritat de control en els casos previstos a l'article 36.1 del RGPD.

d) Vetllar, abans i durant tot el tractament, perquè l'encarregat compleixi la normativa en matèria de protecció de dades.

e) Supervisar el tractament, inclosa l'execució d'inspeccions i auditories.

f) Complir amb el dret d'informació dels afectats

Sisena.- Drets del responsable del tractament:

El responsable del tractament té dret a:

a) Obtenir de l'encarregat tota la informació que consideri necessària relativa a les dades i els tractaments que es descriuen a la clàusula segona, per tal que pugui complir amb les seves obligacions com a responsable.

b) Obtenir l'assistència de l'encarregat per atendre les peticions i inspeccions de qualsevol autoritat de control, quan els tractaments objecte de les mateixes siguin els que porta a terme l'encarregat.

c) Ser compensat per l'encarregat pels danys i perjudicis que suporti com a conseqüència de l'incompliment de les obligacions de l'encarregat o dels seus subcontractats.

inefc Institut Nacional d'Educació Física de Catalunya

Setena.- Modificació de l'Acord

Aquest acord d'encàrrec de tractament es podrà modificar de manera expressa de comú acord entre les parts, mitjançant la signatura de la corresponent addenda.

Vuitena.- Comunicacions i notificacions

Les comunicacions adreçades al responsable del tractament s'enviaran a : Inefc.pd@gencat.cat

Les comunicacions adreçades a l'encarregat del tractament s'enviaran a : protecciondedatos@universitasxxi.com

Novena.- Seguiment i control

Les parts resoldran de comú acord qualsevol controvèrsia o discrepància que pogués sorgir en la interpretació, l'execució i el compliment d'aquest acord.

Qualsevol aspecte que sigui rellevant en el seguiment es comunicarà a l'altra part mitjançant les bústies electròniques especificades a la clàusula vuitena d'aquest acord.

En prova de conformitat, ambdues parts signen electrònicament el present acord, quedant un exemplar en poder de cada una de les parts.

Institut Nacional d'Educació Física de Catalunya

UNIVERSITATS XXI, Soluciones y Tecnología para la Universidad, S.A.

Director

Per suplència:

Josep Vilà i Campanyà
Gerent
(Resolució de 31 de maig de 2023)

Apoderada

Generalitat de Catalunya

Annex 1. Mesures de seguretat. Tractament Expedients acadèmics (risc mitjà)

Naturalesa	Mesura	Descripció Nivell
Mesures d'Organització	Normativa	1. La Normativa de protecció de dades ha de plasmar de forma clara i precisa, almenys, el següent: a) Organització de protecció de dades: - Designació del Delegat de Protecció de Dades (DPD) dels tractaments automatitzats i no automatitzats. - Designació del Comitè o Comitès per a la gestió i coordinació de la protecció de dades, detallant-ne l'àmbit de responsabilitat, els membres i la relació amb altres elements de l'organització. - Designació del Responsable de ciberseguretat i compliment de protecció de dades. - Definició dels rols i funcions definint per a cadascun els deures i responsabilitats. b) Definició de la categorització de cada lloc de treball en matèria de protecció de dades que defineixi les funcions, deures i obligacions del personal; i els criteris i regles d'ús encaminats a la correcta utilització de les eines de treball i els serveis. Ha d'incloure la responsabilitat dels usos indeguts i les mesures disciplinàries associades. c) Model de relació amb l'autoritat de control. d) Registre d'Activitats de Tractament que haurà de contenir com a mínim els següents camps: - Nom i dades de contacte del DPD, del Responsable del Tractament i, si s'escau, del corresponsable i del representant del responsable. - Activitats i finalitats dels tractaments. - Descripció de les categories de dades i dels interessats. - Categories dels destinataris a qui se li han comunicat o comunicaran les dades, inclosos els destinataris en tercers països o organitzacions internacionals. - Transferències internacionals de dades. - Quan sigui possible, els terminis previstos per a la supressió de les diferents categories de dades. - Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat. e) Si s'actua com encarregat del tractament, haurà de portar un registre de les categories d'activitats de tractament que porta a terme per compte d'un responsable que haurà de contenir la següent informació: - Nom i dades de contacte del encarregat i de cada responsable per compte del que actuï i, si s'escau, del representant del responsable o del encarregat i del DPD. - Categories de tractaments efectuats per compte de cada responsable. - Transferències internacionals de dades. - Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat. f) Identificació de les Activitats de Tractament i sistemes d'informació associats. g) Definició dels nivells de risc de les Activitats de Tractament i els criteris per la classificació. h) Metodologia d'Avaluació d'Impacte relativa a la Protecció de Dades (AIPD). i) Identificació de les mesures de ciberseguretat associades als diferents nivells de risc. 2. La normativa referida en aquest apartat haurà de mantenir-se en tot moment actualitzada i serà revisada sempre que es produeixin canvis rellevants. 3. Qualsevol incompliment o excepció de la normativa haurà de ser correctament documentat.
	Procediments	1. S'ha de disposar, com a mínim, dels següents documents que detallin de forma clara i precisa com portar a terme els tractaments automatitzats: a) Control d'accés lògic (gestió d'usuaris). Ha d'incloure el control d'accés a les dades que tenen limitat el tractament. b) Identificació i autenticació. c) Gestió de suports. d) Còpies de seguretat i restauració de dades. e) Control d'accés físic. f) Tractament de fitxers temporals. g) Eliminació segura d'informació en la reutilització o destrucció de suports i sistemes. h) Devolució d'actius. i) Registre d'accessos. j) Gestió d'excepcions. k) Treball fora dels locals del responsable de les Activitats de Tractament o encarregats dels tractaments. l) Notificació, registre i gestió d'incidències. m) Notificació de vulneracions de seguretat. 2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.
		3. S'ha de disposar, com a mínim, dels següents documents que detallin de forma clara i precisa com portar a terme els tractaments automatitzats: a) Pseudonimització.
	Procediments d'autorització	1. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes: a) Ús de dispositius mòbils (ordinadors portàtils, dispositius mòbils intel·ligents, tauletes, agendes electròniques, etc.). b) Ús de suports (dispositius òptics (CD's, DVD's), discs durs externs, cintes i discs de còpies de seguretat, unitats USB o pendrives, targetes de memòria (SD, microSD, etc.)). c) Sortida de dispositius mòbils i suports. d) Tractament fora dels locals del Responsable del Tractament o Encarregat del Tractament. e) Accés remot. f) Execució dels procediments de recuperació de dades. g) Entrada en producció i manteniment d'equips i aplicacions. 2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.
		3. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes: a) Execució del Pla de Continuïtat i les proves periòdiques.
	Deures i obligacions del personal	1. S'ha d'informar al personal de: a) Les funcions, deures i obligacions tant durant el període el qual exerceix el lloc de treball com en cas de finalització de l'assignació o trasllat a un altre lloc de treball. b) Els requisits a complir respecte les dades a les que ha tingut accés, en particular, en termes de confidencialitat, tant durant el període en el qual ha estat adscrit com posteriorment a la seva finalització. c) Les mesures disciplinàries en cas d'incompliment.
	Formació i conscienciació	1. En coordinació amb el DPD, s'han de dur a terme les accions necessàries per formar i conscienciar regularment el personal sobre el seu paper i responsabilitat en matèria de protecció de dades perquè la seguretat dels tractaments automatitzats i no automatitzats assoleixi els nivells exigits. En particular, pel que fa a: a) La normativa, procediments i estàndards de seguretat relativa al bon ús dels sistemes i els tractaments en paper. b) La detecció i reacció a incidents de seguretat, activitats o comportaments sospitosos. c) El procediment de notificació d'incidents i vulneracions de seguretat. d) La gestió de la informació en qualsevol format en què es trobi. S'han de cobrir almenys les activitats següents: llocs de treball endreçats, emmagatzematge, transferència, còpies, distribució, destrucció i ús de fitxers temporals.

Naturalesa	Mesura	Descripció Nivell
	Arquitectura de seguretat	1. S'han de dissenyar i configurar els sistemes i xarxes aplicant la regla de mínima funcionalitat i la seguretat per defecte. 2. El disseny d'arquitectura de seguretat ha de contemplar les instal·lacions, els sistemes, l'esquema de línies de defensa i els sistemes d'identificació i autenticació. 3. S'han de configurar de forma segura els equips, prèviament a al seva entrada en producció de forma que s'apliquin mesures tècniques i organitzatives que garanteixin, per defecte: a) la limitació del tractament de dades per part dels usuaris dels diferents sistemes d'informació d'acord amb les funcions que l'usuari ha de desenvolupar. b) la retirada de comptes i contrasenyes per defecte. c) que no es proporcionin funcions innecessàries, ni d'operació, ni d'administració, ni d'auditoria, de manera que es redueixi el seu perímetre al mínim imprescindible. d) que no es proporcionin funcions que no siguin d'interès , ni siguin necessàries i, fins i tot, les que siguin inadequades al fi que es persegueix. 4. S'ha de mantenir documentació tant del disseny d'arquitectura com de la configuració dels equips. 5. De manera prèvia a l'entrada en producció s'ha de realitzar un anàlisi de vulnerabilitats. 6. S'ha de demanar autorització relativa a l'entrada en producció i manteniment d'equips i aplicacions.
		7. S'ha de formalitzar i documentar el disseny de l'arquitectura de seguretat i la configuració dels equips. 8. La descripció del disseny i configuració ha de contemplar: a) Instal·lacions: nombre, ubicació, àrees existents i detall dels punts d'accés. b) Sistemes: inventari dels sistemes d'informació que, com a mínim, contingui: - Els actius dels sistemes (servidor de correu, robot de backup...). - Les xarxes existents, així com els elements de connexió a l'exterior (p.ex. la xarxa local està separada d'Internet mitjançant un tallafocs). - Els punts d'accés als sistemes (llocs de treball, consoles d'administració, web de la intranet, etc.). c) Esquema de línies de defensa: - Inventari dels sistemes de seguretat (tallafocs, DMZ, antivirus, antispam, etc.). - Elements d'interconnexió a altres sistemes o a altres xarxes. - Elements de defensa en les connexions a altres xarxes (per exemple, la connexió amb Internet es realitza a través d'un tallafocs). - Utilització de tecnologies diferents per prevenir vulnerabilitats que puguin perforar simultàniament diverses línies de defensa. d) Sistema d'identificació i autenticació d'usuaris per a cada sistema o servei: - Ús de claus concertades, contrasenyes, targetes d'identificació, biometria, o altres de naturalesa anàloga. - Ús de fitxers o directoris per autenticar l'usuari i determinar els seus drets d'accés. e) Sistema de gestió, relatiu a la planificació, l'organització i el control dels recursos relatius a la seguretat de la informació. 9. El disseny de l'arquitectura ha d'estar aprovada per la unitat competent del CTTI i assessorat per l'equip d'especialistes en ciberseguretat de l'organisme competent en la matèria de la Generalitat de Catalunya (actualment, el CESICAT) o àrees equivalents de l'organització responsable o encarregada del tractament.
	Desenvolupament segur	1. El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció i no hi ha d'haver eines o dades de desenvolupament en l'entorn de producció. 2. S'ha d'aplicar una metodologia de desenvolupament reconeguda que: a) Prengui en consideració els aspectes de seguretat en tot el cicle de vida. b) Utilitzi algoritmes, programari i biblioteques reconegudes. c) Contempli la generació i el tractament de pistes d'auditoria que permeti registrar les activitats dels usuaris tal i com s'especifica a la mesura Id 20 "Registre i protecció d'activitat dels usuaris". 3. De manera prèvia a l'entrada en producció s'ha de realitzar: a) Comprovació del funcionament correcte de l'aplicació. b) Anàlisi de vulnerabilitats.
		4. S'ha d'aplicar una metodologia de desenvolupament reconeguda que: a) Permeti la inspecció del codi font. b) Permeti comprovar que les dades d'entrada d'un usuari es corresponen a l'esperat (validació de dades d'entrada, sortida i dades intermèdies). 5. De manera prèvia a l'entrada en producció s'ha de realitzar: a) Proves de penetració. b) Anàlisi del codi font.
	Proves	1. Les proves s'han de fer en un entorn aïllat del de producció. 2. Les proves anteriors a l'entrada en producció o modificació no s'han de fer amb dades reals, llevat que s'asseguri que l'entorn en el que es facin les proves tingui implementades les mesures de ciberseguretat establertes pel nivell de seguretat del tractament de les dades.
	Requisits d'accés i segregació de funcions	1. Els requisits d'accés s'han d'atenir al que s'indica a continuació: a) Tot sistema d'informació ha de disposar de mecanismes d'autenticació per a validar la identitat dels usuaris que hi accedeixen. b) Els recursos del sistema s'han de protegir amb algun mecanisme que n'impedeixi la utilització, llevat de les entitats, usuaris o persones que gaudeixin de drets d'accés suficients. c) Els drets d'accés de cada recurs s'han d'establir segons les decisions de la persona responsable del recurs, i s'han d'atenir a la normativa de seguretat del sistema. d) Particularment, s'ha de controlar l'accés als components del sistema i als seus fitxers o registres de configuració.
		2. El sistema de control d'accés s'ha d'organitzar de forma que s'exigeixi la concurrència de dues o més persones (o bé dos rols diferenciats per a cadascuna de les funcions que es duguin a terme) per realitzar tasques crítiques, i que anul·li la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita. En concret, s'han de separar almenys les funcions següents en diferents rols per evitar que una sola persona pugui dur a terme ambdues funcions en relació a un sistema: a) Desenvolupament d'operació. b) Configuració i manteniment del sistema d'operació. c) Auditoria o supervisió de qualsevol altra funció. En especial, es verificarà aquesta separació de rols i funcions en casos d'usuaris administradors i es garantirà que cap administrador ostenta en aquesta condició dues de les funcions definides anteriorment.

I.N.E.F.C.

Naturalesa	Mesura	Descripció Nivell
Mesures de Gestió	Identificació i autenticació	1. Abans de proporcionar les credencials d'autenticació als usuaris, aquests s'han d'haver identificat i registrat de manera fidedigna davant el sistema o davant un proveïdor d'identitat electrònica reconegut per l'Administració. Es preveuen diverses possibilitats de registre dels usuaris: - Mitjançant la presentació física de l'usuari i la verificació de la seva identitat d'acord amb la legalitat vigent, davant un funcionari habilitat per a això. - De manera telemàtica, mitjançant DNI electrònic o un certificat electrònic qualificat. - De manera telemàtica, utilitzant altres sistemes admesos legalment per a la identificació dels ciutadans dels que prevegi la normativa aplicable. 2. Els mecanismes d'autenticació emprats a cada sistema s'han d'adequar al nivell del sistema i respondre als mecanismes autoritzats al Reglament Europeu 910/2014 (eIDAS) i reglaments d'execució del mateix, així com el Protocol d'Identificació i Signatura Electrònica, aprovat per l'Ordre GRI/233/2015, de 20 de juliol, i la Política d'Identificació i Signatura Electrònica del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. Els mecanismes poden utilitzar els factors d'autenticació següents: - "Factors de coneixement": contrasenyes o claus concertades. Han de disposar de regles bàsiques de qualitat (extensió, tipus de caràcters, etc.). - "Factors de possessió": components lògics (com ara certificats de programari) o dispositius físics (tokens, telèfons mòbils, dispositius). - "Factors inherents o propis de l'usuari": elements biomètrics. 3. En l'àmbit bàsic es requerirà com a mínim un factor d'autenticació. Els factors anteriors es poden utilitzar de manera aïllada o combinar-se per generar mecanismes d'autenticació forta (veure nivells superiors). 4. La identificació dels usuaris del sistema s'ha de fer d'acord amb el que s'indica a continuació: a) Els identificadors d'usuari han de complir amb el MCPD i el Marc Normatiu de la Seguretat de la Informació de la Generalitat de Catalunya. b) Es poden utilitzar com a identificador únic els sistemes d'identificació que prevegi la normativa aplicable. c) Quan l'usuari tingui diferents rols davant del sistema (p.ex. com a ciutadà, com a treballador intern de l'organisme i com a administrador dels sistemes), ha de rebre identificadors singulars per a cadascun dels casos de manera que sempre quedin delimitats privilegis i registres d'activitat. d) Cada entitat (usuari o procés) que accedeix al sistema ha de disposar d'un identificador únic de manera que: - Es pot saber qui rep i quins drets d'accés rep. - Es pot saber qui ha fet alguna cosa i què ha fet. 5. Les credencials s'han de gestionar de la manera següent: a) S'han d'activar una vegada estiguin sota el control efectiu de l'usuari. b) Han d'estar sota el control exclusiu de l'usuari. c) L'usuari ha de reconèixer que les ha rebut i que coneix i accepta les obligacions que implica la seva tinença, en particular, el deure de custòdia diligent, protecció de la seva confidencialitat i informació immediata en cas de pèrdua. d) Han de ser inhabilitats en els casos següents: quan l'usuari deixa l'organització per qualsevol causa; quan l'usuari cessa en la funció per a la qual es requeria el compte d'usuari; o quan la persona que el va autoritzar dóna ordre en sentit contrari. En definitiva, quan s'acaba la relació amb el sistema. e) S'han de retenir durant el període necessari per atendre les necessitats de traçabilitat dels registres d'activitat que hi estan associats. A aquest període se'l denomina període de retenció. f) S'han de revisar periòdicament els identificadors i verificar si és necessari que accedeixin als sistemes d'informació. g) En el cas que siguin contrasenyes, s'han de configurar segons l'estàndard de contrasenyes del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. Concretament, en allò referent a la complexitat, longitud, caducitat, limitació del nombre d'intents fallits, reutilització i emmagatzematge. En cas d'utilitzar OTPs aquests no tindran una duració superior a 24 hores.
		6. S'exigeix l'ús d'almenys dos factors d'autenticació de diferent tipologia. En el cas d'utilització de factors de coneixement, s'ha de donar compliment a les exigències de qualitat i renovació establertes al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya, atenent a la tipologia de perfil a què correspon la credencial. 7. Les credencials utilitzades s'han d'haver obtingut després d'una registre previ: a) Mitjançant la presentació física de l'usuari i la verificació de la seva identitat d'acord amb la legalitat vigent, davant un funcionari habilitat per a això. b) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat. c) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat en un dispositiu de creació de signatura.
	Gestió de drets d'accés dels usuaris	1. L'assignació i l'ús dels privilegis d'accés ha d'estar restringida i controlada. L'assignació de drets d'accés privilegiats ha d'estar recollida en un procés formal d'autorització, d'acord amb la normativa de control d'accés aplicable. Només el personal autoritzat pot concedir, alterar o anul·lar l'autorització d'accés als recursos, de conformitat amb els criteris establerts pel seu propietari. 2. Els drets d'accés de cada usuari s'han de limitar atenent els principis següents: a) Mínim privilegi. Els privilegis de cada usuari s'han de reduir al mínim estrictament necessari per complir les seves obligacions. b) Necessitat de conèixer. Els privilegis s'han de limitar de forma que els usuaris només accedeixin al coneixement d'aquella informació requerida per complir les seves obligacions. 3. L'assignació de drets ha de tenir en compte el següent: a) Haurien d'identificar-se els drets d'accés privilegiats associats a cada sistema o procés (p.ex. sistema operatiu, sistema de gestió de BBDD, aplicacions) juntament amb els usuaris als que s'han d'assignar. b) S'ha d'autoritzar l'assignació de privilegis i s'han de registrar tots els privilegis assignats. Els drets d'accés no s'han de fer efectius fins que es completi el procés d'autorització. c) Han de definir-se els requisits per al venciment dels drets d'accés privilegiats. d) Els drets d'accés han d'assignar-se a un identificador d'usuari. e) S'han de revisar periòdicament els permisos assignats als usuaris i, verificar que es corresponen a les seves funcions. f) En cas que sigui recomanable per criteris d'eficiència i no generi riscos de seguretat, l'assignació de permisos d'usuari es podrà realitzar en base a la definició i parametrització de rols, d'acord amb allò establert al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. g) S'han d'establir i mantenir procediments per a evita l'ús no autoritzat de l'identificador d'usuari, en especial pel que fa a aquelles credencials amb permisos d'administrador.
	Accés local i remot	Es considera accés local el realitzat des de llocs de treball dins de les mateixes instal·lacions de l'organització i des dels recursos propis ubicats en dites instal·lacions. Es considera accés remot el realitzat des de fora de les mateixes instal·lacions de l'organització, a través de xarxes o recursos de tercers que no estiguin posats a disposició específicament com a recursos locals o propis de la Generalitat de Catalunya. 1. S'ha de garantir la seguretat del sistema quan hi accedeixin remotament usuaris o altres entitats, cosa que implica protegir tant l'accés en si mateix com el canal d'accés remot. La concepció d'accés remot s'haurà d'aplicar a les formes establertes de Teletreball al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. 2. Els accessos hauran de complir amb les següents mesures segons el nivell dels tractaments: a) S'han de prevenir atacs que puguin revelar informació del sistema sense arribar a accedir-hi. La informació revelada a qui intenta accedir-hi ha de ser la mínima imprescindible (els diàlegs d'accés només han de proporcionar la informació indispensable). b) El sistema ha d'informar l'usuari de les seves obligacions, si fossin específiques, immediatament després d'obtenir l'accés. Aquesta informació en relació amb les obligacions generals aplicables als sistemes de la Generalitat es mostrarà la primera vegada que l'usuari accedeixi al sistema. c) Passat un cert temps d'inactivitat en la sessió de l'usuari, ja sigui amb el sistema o amb una aplicació en particular, s'han de cancel·lar les sessions obertes des de l'esmentat lloc de treball. 3. S'aplicaran a les connexions en remot les mesures de seguretat establertes per a l'accés local, sempre i quan resultin adients. En cas contrari es definiran mesures equivalents per a assolir un nivell de seguretat equiparable.
		4. S'ha d'informar l'usuari de l'últim accés efectuat amb la seva identitat. 5. S'ha d'establir una política específica del que es pot fer remotament, per a la qual cosa es requereix autorització positiva. 6. Quan un equipament es connecti remotament a través de xarxes que no estan sota el control estricte de l'organització, l'àmbit d'operació del servidor ha de limitar la informació i els serveis accessibles als mínims imprescindibles i, s'ha de requerir una autorització prèvia dels responsables dels tractaments de dades afectats. Aquest punt és aplicable a connexions a través d'Internet i altres xarxes que no siguin de confiança.

Naturalesa	Mesura	Descripció Nivell
	Contractació i acords de nivell de servei	1. S'han de subscriure, si són d'aplicació els escenaris descrits, els següents contractes o altres actes jurídics amb els següents actors: a) Encarregats del Tractament. Aquests han d'establir de forma clara i concisa, com a mínim: - Objecte. - Durada. - Naturalesa i finalitat del tractament (característiques del servei prestat). - Tipus de dades personals. - Categoria dels interessats. - Obligacions, responsabilitats i drets del Responsable. - Obligacions, responsabilitats i drets de l'Encarregat segons el clausulat de l'article 28.3 RGPD. - Mesures tècniques i organitzatives que ofereixin unes garanties suficients d'acord amb el nivell de risc de les dades. - Nivells de servei (temps de resposta en cas de violacions de seguretat, resolució d'incompliments, etc.). - Conseqüències de l'incompliment. - Devolució o destrucció de les dades a la finalització de l'encàrrec. b) Prestadors de serveis sense accés a dades. Aquests han d'establir de forma clara i concisa, com a mínim: - Naturalesa i finalitat del servei. - Prohibició d'accedir a les dades personals. - Obligació de deure de secret respecte a les dades que el personal hagués pogut conèixer amb motiu de la prestació de servei. - Conseqüències de l'incompliment. 2. Els Encarregats del Tractament han de subscriure contractes o altres actes jurídics amb els subencarregats que utilitzin per a dur a terme determinades activitats de tractament. Aquests hauran d'establir, com a mínim, les mateixes obligacions de protecció que les estipulades en el contracte o altre acte jurídic entre el responsable i l'encarregat. Les subcontractacions han d'estar autoritzades pel Responsable del Tractament. 3. El Responsable del tractament ha d'identificar les activitats dels tractaments i sistemes d'informació tractats per compte de tercers amb referència expressa a l'encarregat, al contracte o document que reguli les condicions i la vigència de l'encàrrec. 4. Si s'actua com Encarregat del Tractament s'ha d'identificar i registrar les activitats de tractament i sistemes d'informació que tracta per compte de tercers, si és el cas, amb referència expressa al Responsable del tractament, al contracte o document que reguli les condicions i la vigència de l'encàrrec. 5. En cas de disposar d'encarregats de tractament el Responsable haurà d'establir un sistema de garanties per acreditar la qualitat i adequació professional de l'encarregat de tractament. Aquest s'haurà d'introduir en els models d'acreditació de la solvència tècnica en els procediments de contractació i es podrà basar en l'acreditació professional mitjançant certificats i models de compliment voluntaris (com per exemple codis de conducta) reconeguts a nivell nacional i/o internacional.
		6. Els contractes o actes jurídics hauran de preveure l'auditabilitat dels sistemes d'informació per a verificar el nivell de compliment de les mesures de ciberseguretat. 7. Els contractes hauran de preveure la revisió de les condicions de tractament. 8. Establiment d'un sistema rutinari per mesurar el compliment de les obligacions de servei que inclogui un procediment per neutralitzar qualsevol desviació respecte el contracte.
	Condicionament dels locals	1. Els locals on s'ubiquin els sistemes d'informació i els seus components han de disposar d'elements adequats per al funcionament eficaç de l'equipament instal·lat allà. I, especialment: a) Condicions de temperatura i humitat. b) Energia elèctrica, i les seves preses corresponents, necessària per a funcionar, de forma que es garanteixi el subministrament de potència elèctrica i el funcionament correcte dels llums d'emergència. c) Protecció contra les amenaces identificades a l'anàlisi de riscos. d) Protecció del cablatge contra incidents fortuïts o deliberats. 2. S'ha de garantir el subministrament elèctric als sistemes en cas de fallada del subministrament general i garantir el temps suficient perquè finalitzin ordenadament els processos, salvaguardant la informació.
	Control d'accés físic	L'equipament s'ha d'instal·lar en àrees específiques per a la seva funció (àrees de CPDs o sales tècniques, edificis o ubicacions on es trobi ubicat aquest equipament). S'han de controlar els accessos a les àrees indicades de manera que només s'hi pugui accedir per les entrades previstes i vigilades. 1. Han de quedar registrades l'entrada i sortida de les persones a les àrees separades i concretament la identificació de la persona, la data i hora d'entrada i sortida. 2. El registre d'accessos ha d'estar controlat per una persona autoritzada.
	Registre d'entrada i sortida d'equipament i suports	S'ha de garantir que l'equipament i els suports estan sota control i que satisfan els seus requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. A aquest efecte: 1. S'ha de portar un registre detallat de qualsevol entrada i sortida d'equipament i suports dels CPDs, sales tècniques, edificis o ubicacions on es trobin aquests equipaments o suports, incloent-hi la identificació de la persona que autoritza el moviment. El registre ha de reflectir: data i hora, identificació inequívoca de l'equipament, persona que realitza l'entrada o sortida, persona que autoritza l'entrada o sortida i persona que realitza el registre. 2. S'ha d'elaborar una llista de serveis autoritzats de transport o missatgeria a emprar. 3. S'ha de disposar d'un procediment informal que compari les sortides amb les arribades per tal de detectar algun incident.
		4. El procediment previst en nivell bàsic que compari semestralment les sortides amb les arribades ha de ser rutinari, formal i que dispari les alarmes pertinents quan es detecti algun incident.
	Controls d'auditoria dels sistemes de la informació	1. El Responsable de tractament haurà de tenir un model de compliment que permeti el seguiment, revisió i autoavaluació de les mesures de seguretat aplicades als tractament de dades de caràcter personal. Aquest model de compliment ha de permetre acreditar i disposar de les evidències pertinents per acreditar el nivell de compliment en relació amb el present MCPD o amb les mesures excepcionals que s'hagin determinat a les corresponents AIPD.
		2. Els sistemes d'informació que suporten els tractaments de dades personals seran objecte d'auditories parcials o totals que es realitzaran en virtut d'una planificació que respongui als resultats del seguiment, revisió i autoavaluació de les mesures de seguretat. 3. Les auditories podran ser internes o externes però les persones que les portin a terme hauran de ser independents i expertes. 4. Les auditories es realitzaran segons els criteris i estàndards establerts pel CESICAT. 5. L'informe d'auditoria dictaminarà el grau de compliment de les mesures establertes en aquest Marc segons l'abast que es determini i les seves conclusions s'hauran de presentar al Responsable del Tractament.
	Registre i protecció de l'activitat dels usuaris	1. S'han de registrar les activitats dels usuaris en el sistema, de manera que: a) El registre ha d'indicar qui fa l'activitat, quan la fa i sobre quina informació i les activitats efectuades amb èxit i els intents fallits. b) S'ha d'incloure l'activitat dels usuaris i, especialment, la dels operadors i administradors quan puguin accedir a la configuració i actuar en el manteniment del sistema. c) La determinació de quines activitats s'han de registrar i amb quins nivells de detall s'han d'adoptar en vista de l'anàlisi de riscos feta sobre el sistema i les capacitats del mateix. 2. S'han d'activar els registres d'activitat en els servidors. 3. El període de conservació de la informació es regirà per la normativa de gestió de traces del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya (18 mesos). 4. En cas de produir-se incidents o un increment de risc en relació amb amenaces o bé es produeix un requeriment de caràcter legal, es podrà recuperar, revisar i analitzar la informació associada a aquesta activitat sempre aplicant criteris de necessitat, idoneïtat i proporcionalitat.
		5. S'han de revisar informalment els registres d'activitat per buscar patrons anormals. A aquest efecte, es podrà disposar d'eines específiques automàtiques destinades a l'anàlisi d'aquests patrons per tal de determinar potencials incompliments. En cas de detectar-se podran analitzar-se en detall les dades que han generat la detecció d'aquests patrons atenent a l'amenaça i al nivell de risc. Aquestes eines podran ser transversals i/o operades per organismes específics dedicats a la ciberseguretat.
		1. S'ha d'establir un registre d'incidents en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes derivats i les mesures correctores aplicades. A mes, s'hauran de registrar les restauracions de còpies de seguretat, indicant la persona que realitza el procés, les dades restaurades i les dades que 'hagin hagut de gravar manualment en el procés de recuperació.

Naturalesa	Mesura	Descripció Nivell
Mesures de Protecció	Gestió d'incidents i sistema de notificacions d'incidents	2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que: a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident. b) S'ha de registrar l'evidència que pugui sostenir, posteriorment, una actuació legal (administrativa o judicial), o fer-hi front, quan l'incident pugui portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes. En la determinació de la composició, detall i gestió d'aquestes evidències, s'ha de recórrer a assessorament legal especialitzat. c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments. 3. S'ha d'assegurar que es disposi de la informació necessària per fer la notificació d'informació en els termes previstos al Reglament General de Protecció de dades. És a dir, s'haurà de poder facilitar la següent informació referent a les vulneracions de seguretat de les dades personals: a) Descripció de la naturalesa de la vulneració de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats. b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals. c) Descripció de les mesures adoptades o proposades pel responsable del tractament per fer front a la vulneració de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.
	Inventari d'actius	1. S'han de mantenir inventaris actualitzats de tots els elements del sistema (informació, programari, maquinari, serveis, tercers, persones, instal·lacions, suports d'informació), detallant-ne com a mínim: a) El responsable. b) Tipus d'actiu (servidor, ordinador, router, etc.). c) Identificador, fabricant i model. d) Ubicació. 2. Els inventaris s'actualitzaran en funció dels terminis establerts a la normativa.
	Fitxers temporals	1. Els fitxers temporals que s'haguessin creat exclusivament per la realització de treballs temporals auxiliars hauran de complir amb les mesures establertes que s'apliquin als fitxers considerats definitius. 2. Tot fitxer temporal així creat serà esborrat una vegada hagi deixat de ser necessari per la finalitat que va motivar la seva creació.
	Protecció d'equips	1. El lloc de treball s'ha de bloquejar al cap d'un temps prudencial d'inactivitat i ha de requerir una nova autenticació de l'usuari per reprendre l'activitat en curs. 2. Els equips han de disposar de protecció antivirus i antimalware. 3. Els equips que siguin susceptibles de sortir de les instal·lacions de l'organització i no es puguin beneficiar de la protecció física corresponent, amb un risc manifest de pèrdua o robatori, s'han de protegir adequadament. Sense perjudici de les mesures generals que els afectin, s'ha d'evitar, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideren claus d'accés remot les que siguin capaces d'habilitar un accés a altres equips de l'organització, o altres de naturalesa anàloga.
	Manteniment d'equipament	S'han d'aplicar les mesures preventives i correctives necessàries per a mantenir l'equipament físic i lògic assegurant la confidencialitat, integritat i disponibilitat continua dels equips i sistemes. D'acord amb això, s'ha de disposar de: 1. Les especificacions dels fabricants pel que fa a la instal·lació i manteniment dels sistemes. 2. Un seguiment continu dels anuncis de defectes, utilitzant mecanismes, com per exemple, la subscripció de correu d'avisos de defectes per part del fabricant. 3. Un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pedaços, millores i noves versions.
	Protecció dels suports d'informació	1. Els suports d'informació s'han d'identificar mitjançant etiquetatge o mecanisme equivalent de forma que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de més qualificació. 2. Les etiquetes o mecanismes equivalents haurien de ser fàcilment identificables. S'informarà als usuaris sobre aquests mecanismes d'identificació per tal que, o bé mitjançant simple inspecció, o bé mitjançant el recurs a un repositori, puguin entendre el significat. 3. Es podrà excloure, per previsió a la normativa, l'obligació d'etiquetatge en cas de suports en que no es pogués complir per les seves característiques físiques, establint mesures alternatives per assegurar la seva identificació i localització. 4. Els suports d'informació que s'hagin de reutilitzar per a una altra informació o lliurar a una altra organització han de ser objecte d'un esborrament segur del seu contingut.
		5. S'han de destruir de manera segura els suports d'informació, en els casos següents: a) Quan la naturalesa del suport no permeti un esborrat segur. b) Quan així ho requereixi el procediment associat al tipus d'informació continguda. 6. S'han d'aplicar mecanismes criptogràfics que garanteixin la confidencialitat i la integritat de la informació continguda en tots els suports.
	Devolució d'actius	El personal intern o extern haurà de retornar tots els actius de l'organització que estiguin en el seu poder al finalitzar la relació laboral, el contracte o acord.
	Protecció del lloc de treball	1. S'ha d'exigir que els llocs de treball estiguin endreçats, sense més material damunt la taula que el requerit per a l'activitat que es realitza en cada moment.
		2. El material s'ha de guardar en un lloc tancat quan no s'utilitzi. S'haurà de disposar de llocs tancats a disposició dels usuaris.
	Limitació del tractament de dades personals	Un cop finalitzi el tractament de dades i quan el Responsable del tractament hagi establert que les dades personals s'han de conservar pels motius establerts al RGPD o a la legislació aplicable, que impliquin una limitació d'ús de les mateixes, s'hauran d'adoptar mesures tècniques per protegir les dades d'acord amb aquest nou estat, com les següents: 1. Control d'accés. 2. Ubicació de les dades en un sistema diferent. 3. Xifrat.
	Còpies de Seguretat	1. S'han de fer còpies de seguretat que permetin recuperar dades perdudes, accidentalment o intencionadament amb una antiguitat determinada. En particular, s'ha de considerar la conveniència o necessitat, segons que correspongui, que les còpies de seguretat estiguin xifrades. 2. Aquestes còpies han de tenir el mateix nivell de seguretat que les dades originals. 3. Les còpies de seguretat han d'incloure: a) Informació de treball de l'organització que es refereixi a dades personals. b) Aplicacions en explotació, incloent-hi els sistemes operatius mitjançant les que es tractin dades personals. c) Claus utilitzades per preservar la confidencialitat de les dades. 4. Semestralment es verificarà la correcta definició, funcionament i aplicació dels procediments de realització de les còpies i dels procediments de recuperació. 5. La recuperació de còpies haurà de ser autoritzada pel Responsable del tractament.
		6. Les còpies de seguretat i els procediments de recuperació han d'estar emmagatzemats en una ubicació diferent d'aquella en la que es trobin els equips que tracten les dades.
	Pseudononimització	1. En cas de transmissió de dades tant a nivell intern de l'organització com quan sigui a entitats externes a la mateixa o en situacions i contexts de tractament que es considerin sensibles, s'utilitzaran tècniques de pseudonimització o d'altres mesures anàlogues, com el xifrat. 2. Les tècniques de pseudonimització han d'incloure com a mínim: a) Que els atributs estiguin lligats a àlies aleatoris i que no siguin suficients per identificar l'interessat a qui es refereixen. b) L'assignació d'àlies és tal que no es pot revertir sense esforços desproporcionats de les parts interessades.
	Control d'accés a la documentació	1. S'han de limitar els accessos dels usuaris únicament als recursos necessaris per al desenvolupament de les seves funcions. A tal efecte, el Responsable del tractament ha d'elaborar una relació actualitzada d'usuaris i perfils d'usuaris i els accessos autoritzats per a cadascun d'ells.
		2. El Responsable del tractament haurà de definir i establir mecanismes que permetin identificar els accessos realitzats quan els documents puguin ser utilitzats per múltiples usuaris.
	Custòdia, emmagatzematge i destrucció	1. S'ha de disposar de mesures físiques o lògiques, o ambdues, que obstaculitzin la obertura dels dispositius d'emmagatzematge que continguin dades de caràcter personal. Si no és possible adoptar aquesta mesura el responsable del tractament haurà d'adoptar mesures que impedeixin l'accés de persones no autoritzades. 2. Si, per trobar-se en procés de tramitació o revisió, la documentació no es troba arxivada als dispositius d'emmagatzematge escaients, la persona que es trobi al càrrec de la mateixa haurà de custodiar la documentació impedint l'accés a qualsevol persona no autoritzada. 3. S'ha d'exigir que els llocs de treball estiguin endreçats, sense més documentació damunt la taula que la requerida per a l'activitat que es realitza en cada moment. 4. S'ha de destruir qualsevol document que contingui dades de caràcter personal que sigui rebutjat. 5. La destrucció es durà a terme mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació continguda en els mateixos o la seva recuperació posterior per a eliminar el risc d'accés indegut.

Naturalesa	Mesura	Descripció Nivell
	Còpia i reproducció de documents	1. S'han de destruir les còpies o reproduccions rebutjades de manera que s'eviti l'accés a la informació continguda en les mateixes o la seva recuperació posterior.
		2. S'ha de limitar únicament al personal autoritzat pel responsable del tractament la generació de còpies o la reproducció de documents.
	Trasllat de documentació	1. Quan el tractament de dades es realitzi fora dels locals del responsable o de l'encarregat del tractament el responsable del tractament ho haurà d'autoritzar prèviament. 2. S'ha de portar un registre detallat de qualsevol entrada i sortida de documentació. El registre ha de reflectir: data i hora, identificació de la documentació, el nombre de documents, el tipus d'informació que contenen, persona que realitza l'entrada o sortida, la forma d'enviament, la persona que autoritza l'entrada o sortida i la persona que realitza el registre.
		3. S'han d'adoptar mesures dirigides a impedir l'accés a la informació objecte del trasllat o a la seva manipulació.
	Criteris d'arxiu	1. S'ha de garantir la correcta conservació dels documents, la localització i consulta de la informació de conformitat amb els criteris previstos a la legislació vigent sobre arxivística. Aquests criteris han possibilitar l'exercici dels drets previstos a la normativa de protecció de dades. En aquells casos en els quals no existeixi normativa aplicable, el responsable del tractament haurà d'establir els criteris i procediments d'actuació que hauran de seguir-se en matèria d'arxiu.
	Gestió d'incidents i sistema de notificacions d'incidents - paper	1. S'ha d'establir un registre d'incidents en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes derivats i les mesures correctores aplicades.
		2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que: a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident. b) S'ha de registrar l'evidència que pugui sostenir, posteriorment, una actuació legal (administrativa o judicial), o fer-hi front, quan l'incident pugui portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes. En la determinació de la composició, detall i gestió d'aquestes evidències, s'ha de recórrer a assessorament legal especialitzat. c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments. 3. S'ha d'assegurar que es disposi de la informació necessària per fer la notificació d'informació en els termes previstos al Reglament Europeu de Protecció de dades. Es a dir, s'haurà de poder facilitar la següent informació referent a les vulneracions de seguretat de les dades personals: a) Descripció de la naturalesa de la vulneració de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectats. b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals. c) Descripció de les mesures adoptades o proposades pel responsable del tractament per fer front a la vulneració de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.
	Procediments - paper	1. S'ha de disposar dels següents procediments pels tractaments no automatitzats: a) Treball fora dels locals del responsable de les activitats dels tractaments o encarregats dels tractaments. b) Notificació, registre i gestió d'incidències. c) Control d'accés. d) Criteris d'arxiu. e) Dispositius d'emmagatzematge. f) Custòdia. g) Còpia o reproducció. h) Trasllat. i) Destrucció paper.
		j) Registre accés.

I.N.E.F.C.