PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS DEL CONTRACTE DE MANTENIMENT, EVOLUTIUS I ALLOTJAMENT DEL WEB AOC

ÍNDEX

1. OBJECTE DEL CONTRACTE

1.1 Objecte del contracte

El Consorci AOC necessita contractar els serveis de manteniment, suport, evolutius i allotjament dels webs corporatius del Consorci AOC.

Per a que les webs puguin funcionar de forma correcta necessitem un manteniment, desenvolupar evolutius per noves necessitats o modificacions de les actuals, així com una allotjament especialitzat en aquests tipus de webs.

L'AOC necessita un allotjament web especialitzat en Wordpress per tal de garantir l'òptim funcionament de les seves webs corporatives (creades amb aquesta tecnologia) així com un elevat grau de disponibilitat i rendiment i, per tant, de qualitat del servei ofert als nostres usuaris.

1.2 Abast

L'abast del contracte és el següent:

- Manteniment dels webs corporatius: en el dia a dia es requereix d'un manteniment per solucionar els possibles problemes que vagin sortint, mantenir al dia les actualitzacions del Wordpress, etcètera.
- Evolutius dels webs corporatius, com per exemple, desenvolupament o adaptació de nous plugins amb noves funcionalitats, plantilles, etcètera.
- Allotjament dels webs corporatius a un especialitzat en Wordpress.
- Gestió de campanyes de correu electrònic: El gestor de continguts Wordpress està integrat amb una solució de mercat de gestió de campanyes de correu electrònic (actualment Mailchimp) per a l'enviament d'un butlletí amb les novetats del blog i d'avisos de les incidències de serveis. Les tasques d'integració estan fora de l'abast d'aquest contracte. Les tasques d'adaptació dels continguts de Wordpress per a facilitar aquesta integració sí estan incloses en aquest contracte.

Aquestes són les instàncies que en principi necessitarem, encara que en un futur podria sortir la necessitat d'alguna altre:

- Producció:
    - aoc.cat
    - governdigital.cat
    - innovacio.aoc.cat
- Preducció:
    - aoc.cat
- Entorn de proves o LAB: algún entorn que ens serveixi com a laboratorio per fer proves de futurs projectes.

1.3 Indicadors

A continuació mostrem les dades d'us del web que recollim a través de Google Analytics:

Es pot veure que hem tingut gairebé 5,5 milions de visites, però també es pot observar que a la segona meitat de l'any han augmentat considerablement.

En aquest gràfic podem veure la evolució a dos anys:

Visites a pàgines dels darrers mesos:

Abril: 510.168

Maig: 855.258

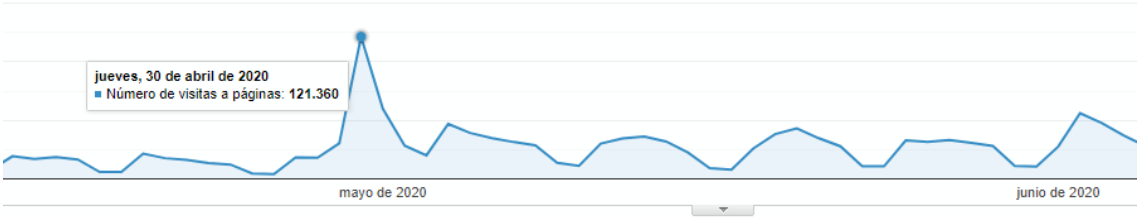
Juny: 759.475

Juliol: 556.250

Agost: 349.318

Setembre: 587.781

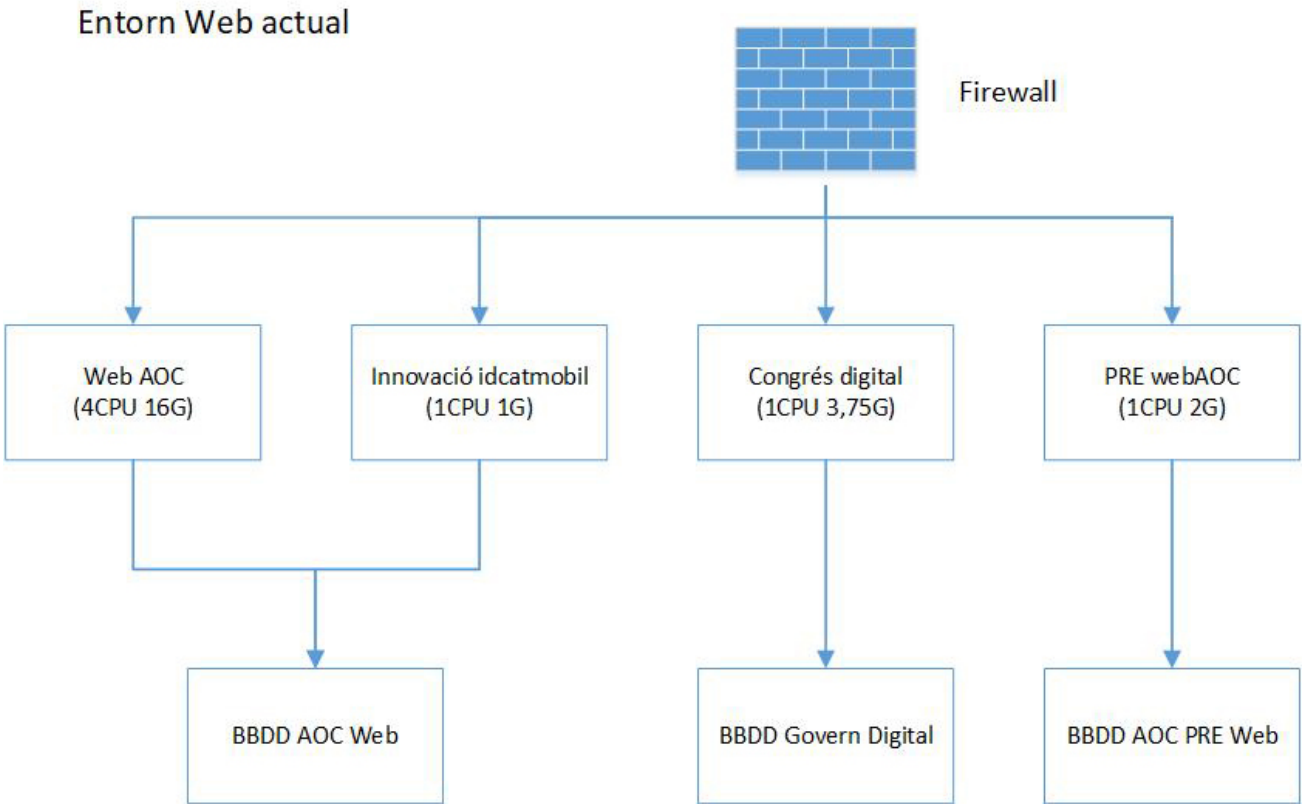
S'ha de tenir en compte que podem tenir pics puntuals de moltes visites, com va passar el 30 d'abril que vam tenir 121.360.



1.4 Infraestructura actual

Actualment tenim un Wordpress amb la darrera versió d'aquest gestor de continguts amb 87 plugins instal·lats, encara que pel proper any s'està executant un contracte per refer de nou el web i l'objectiu és minimitzar el número de plugins.

Esquema amb l'estructura actual del web:



Les webs referides són:

1. AOC: www.aoc.cat, I el seu entorn de preproducció
2. Innovacio: innovacio.aoc.cat
3. Congrés digital: governdigital.cat

Aquestes webs actualment estan instal·lades a un AWS (Amazon Web Services) amb les següents característiques:

Instancies EC2

Nom	Instància	Status	Recursos
PRE Web AOC	t2.small	running	1CPU 2G
Web AOC	t2.xlarge	running	4CPU 16G
Innovació i Idcatmobil	t2.micro	running	1CPU 1G
Congrés digital	m3.medium	running	1CPU 3,75G

Bases de dades

Nom	Instància	Status	CPU	Tipus
aoc-web	db.t2.medium	Available	0.83%	MySQL Community
aoc-preproduccio-web	db.t2.medium	Available	1.17%	MySQL Community
governdigital	db.t2.micro	Available	2.03%	MySQL Community

2. REQUISITS DE LA PRESTACIÓ DEL SERVEI

2.1 Serveis professionals

Els serveis professionals de manteniment i desenvolupament d'evolutius han de complir amb els següents requisits:

Requisits de manteniment i evolutius dels webs
R 1. Manteniment i evolució del web www.aoc.cat (tecnologia Wordpress) a nivell tecnològic (no s'inclou la generació de continguts).
R 2. Optimització del rendiment de la plataforma i del posicionament dels continguts.
R 3. Migració dels webs a un nou centre de dades (si escau)
R 4. Creació, personalització i manteniment d'extensions de Wordpress (plugins) segons les necessitats que sorgeixin.
R 5. Disseny, personalització i manteniment plantilles de Wordpress (temes)
R 6. Web Services amb altres eines corporatives com l'eina de gestió de les peticions de suport.
R 7. Integració amb Mailchimp, SurveyMonkey i les eines que el Consorci AOC determini, del web AOC (p.e. programació d'enviament de butlletins de notícies del Bloc).
R 8. Accessibilitat: els desenvolupaments que es facin hauran de complir amb els criteris d'accessibilitat AA de les WCAG 2.1, com marca la llei.

R 9. Llicències de les extensions (plugins) de Wordpress que necessitin els webs per funcionar segons les necessitats acordades.
R 10. Llicències de serveis de cerca avançada de Google

2.2 Serveis tecnològics i altres

Per a la prestació dels serveis professionals caldrà disposar d'un conjunt de serveis tecnològics que es detallen a continuació.

2.2.1 Servei d'allotjament dels webs corporatius

El servei objecte del contracte ha de complir amb els següents requisits:

Requisits d'allotjament dels webs corporatius
R 11. Monitorització: Monitoratge avançat 24x7 en quant a: RAM, CPU, Apache, etc. Revisió proactiva per part del proveïdor i actuacions consensuades en conseqüència de les dades observades. Revisions de virus, llistes negres, etc, que permetin mantenir la neta la IP. Panell de control on poder veure tots els processos. Estadístiques d'us.
R 12. Disposar d'una política d'accessos a la informació i al servei basada en accessos nominals i contrasenyes amb paràmetres de complexitat i caducitat.
R 13. Disposar del següents elements de seguretat de xarxes: segmentació de xarxes, sistema de firewalls perimetrals.
R 14. S'han de registrar les activitats dels usuaris en el sistema.
R 15. Sistema de copies de seguretat amb les mateixes condicions de seguretat que les dades originals. Les còpies de seguretat hauran de permetre un RPO mínim de 24h.
R 16. Revisió periòdica de vulnerabilitats dels sistemes i disposar d'una política de gestió de vulnerabilitats on es tractin les vulnerabilitats trobades.
R 17. 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: condicions de temperatura i humitat, subministrament elèctric, control d'accessos.
R 18. Alertes: Sistema d'alertes 24x7 respecte HTTP, MySQL, FTP, espai de disc, SMTP, SSH, etc. Tècnics de guàrdia per l'atenció de les alertes 24x7. Notificació d'incidents de seguretat.
R 19. Suport directe d'administradors de sistemes en: Revisió del monitoratge preventiu i proactiu. Actualitzacions de software per millores de rendiment o per detecció de bugs. Restauració de còpies de seguretat. Regles de Firewall a mida. Assessorament. Detecció de millores i optimitzacions
R 20. Seguretat: Compliment de la normativa RGPD.
R 21. Optimitzacions: propostes d'optimització per PageSpeed, processos PHP, etc.

R 22.	Subcontractació: Informació detallada dels subcontractats. Avisos de canvis en la subcontractació
R 23.	Entorns de Producció: web AOC, congrés govern digital i Innovació
R 24.	Entorn de Pre / Proves
R 25.	Dimensionament del servei de d'allotjament de Producció El servei ha d'estar dimensionat, d'entrada, per als següent requeriments mínims: ○ 50.000 visualitzacions de pàgines al dia ▪ Nota: El web AOC no allotja vídeos, ni imatges pesades ○ Temps de resposta mig de les pàgines: 4 segons ○ Capacitat d'atendre de pics de demanda de servei excepcional: fins a 200.000 visualitzacions de pàgines al dia, durant 3% del temps de contracte i garantint la qualitat de servei
R 26.	Dimensionament del servei de d'allotjament de Preproducció / Proves El servei ha d'estar dimensionat, d'entrada, per als següent requeriments: ○ Màxim de 1.000 visualitzacions de pàgines al dia ▪ Nota: El web AOC no allotja vídeos, ni imatges pesades ○ Temps de resposta mig de les pàgines: 5 segons

2.2.2 Requisits de seguretat

2.2.2.1 Requisits de seguretat generals

R 27. Per tal de preservar i poder garantir la seguretat de les dades, la transferència de dades entre el Consorci AOC i l'adjudicatari serà sempre per canals xifrats punt a punt o amb les dades xifrades.

R 28. Les dades del Consorci AOC i els sistemes de tractament de les mateixes estaran ubicades en sales especialment habilitades per tal efecte, amb control d'accés físics i sistemes de control de temperatura i humitat.

R 29. Està prohibit transferir dades del Consorci AOC a suport portàtils, així com el tractament de dades des d'equips portàtils. En cas d'haver de fer-ho, caldrà demanar permís aAOC i xifrar les dades en els suports portàtils.

2.2.2.2 Requisits de seguretat allotjament web

R 30. Durant el temps d'execució del contracte, el licitador haurà d'implantar les mesures de seguretat de sistemes de nivell baix de l'ENS, i que estan indicades al document annex "ANNEX I - Mesures seguretat nivell BAIX.xlsx". Per acreditar que es compleixen les mesures de seguretat l'adjudicatari haurà d'aportar la declaració de conformitat en sistemes de categoria baixa, que l'adjudicatari podrà fer mitjançant una autoavaluació.

El format i contingut de la declaració de conformitat haurà de respectar lo disposat a la Resolució del 13 d'octubre de 2016, Annex 1 i 2, publicat en el BOE a la següent URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10109

2.3 Anàlisis tècnic de seguretat inicial de la infraestructura i solució

Previ a la posada en marxa del servei, el Consorci AOC podrà realitzar un anàlisi tècnic de seguretat inicial de la infraestructura i la solució, per a garantir el compliment dels requisits especificats.

2.4 Normativa aplicable

L'adjudicatari es compromet a que els serveis i sistemes d'informació que proposi compliran la següent normativa i requisits en relació a:

- Les normes ISO/UEC/UNE 17799 de millors pràctiques de seguretat de la informació i UNE71502 de gestió de la seguretat de la informació, adaptades a l'estructura administrativa, personal i entorn tecnològic del client i aplicades de forma proporcional als riscos reals.
- També es compromet a aplicar les mesures, processos i requisits que el client sol·liciti per millorar la qualitat i seguretat i proposar-li els que consideri necessaris per millorar les solucions.
- Es compromet a realitzar, l'anàlisi dels requisits del sistema, la funció de donar suport metodològic i documentar el resultats de l'anàlisi dels riscos del sistema i de la classificació de la criticitat i sensibilitat de les dades i processos. Aquesta anàlisi inclourà també el suport metodològic i la documentació de la classificació de les dades personals en els nivells establers per l'Esquema Nacional de Seguretat, i es prestarà especial atenció al compliment del Reglament General de Protecció de Dades (UE) 2016/679, durant tot el desenvolupament dels treballs.
- Pel que fa al disseny del sistema, es definiran els controls sobre seguretat, incloent-hi, entre d'altres, els controls de compliment del l'Esquema Nacional de Seguretat i el Reglament General de Protecció de Dades (UE) 2016/679, i l'actualització dels plans de contingències i continuïtat. També es realitzarà la prova dels controls de seguretat.
- La Directiva (UE) 2016/2102, del Parlament Europeu i del Consell, de 26 d'octubre de 2016, sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils dels organismes del sector públic, transposada a l'ordenament jurídic al Reial Decret 1112/2018, de 7 de setembre.

3. MILLORES ALS REQUISITS

3.1 Millores dels requisits funcionals, tècnics i de SLA

A part de les prestacions recollides en aquest document es valoraran totes aquelles prestacions superiors o complementaries a les exigides que les empreses licitadores proporcionin en les seves ofertes i que es considerin de valor afegit per a facilitar la gestió del servei.

Els àmbits d'aquestes millores addicionals estan concretats en el Plec de clàusules administratives particulars, apartat de Criteris de Valoració (H2).

4. CLASSIFICACIÓ DE LA INFORMACIÓ I EL SERVEI

Per determinar les mesures de seguretat aplicables per protegir les dades i el servei, s'ha classificat la informació i el servei en funció del valor que aquesta té per a l'organització.

La classificació del sistema s'ha fet seguint les guies de Agència Catalana de Ciberseguretat i del Esquema Nacional de Seguridad.

Segons la guia GUIT049-C del Agència Catalana de Ciberseguretat, la classificació de la informació es pot mesurar en 5 nivells (Molt crític, Crític, Sensible, Intern i Públic) i la classificació del servei en 4 nivells (Essencial, Estratègic, Important i Bàsic).

Denominació del subsistema	**Servei (Disponibilitat)**	**Informació (Seguretat)**	**RTO/RPO**
Web AOC	Bàsic	Públic	2 dies/1 dia
Web Innovació	Bàsic	Públic	5 dies/1 dia
Web Congrés Digital	Bàsic	Públic	5 dies/1 dia
Valor màxim registrat	**Bàsic**	**Públic**	**2 dies/1 dia**

La classificació del sistema segons el Esquema Nacional de Seguridad s'ha fet seguint la guia CCN-STIC 803. Segons aquesta metodologia la classificació del sistema es pot mesurar en 3 nivells (Alt, Mig i Baix).

La classificació del servei segons aquesta metodologia és:

Denominació del subsistema	**Tipus**	**C**	**I**	**D**	**A**	**T**	**DP**
Web AOC	Info i servei	NA	B	B	B	B	N/A
Web Innovació	Info i servei	NA	B	B	B	B	N/A
Web Congrés Digital	Info i servei	NA	B	B	B	B	B
Valor màxim registrat		NA	B	B	B	B	B
La valoració del sistema és Baixa (C=NA, I=B, D=B, A=B, T=B, DP=B)							

Les mesures de seguretat a aplicar per mitigar els riscos segons la classificació es detallaran en el subencàrrec de tractament de dades a signar per l'adjudicatari. En l'annex "Marc de Ciberseguretat de Protecció de Dades: mesures mitigatories identificació remota" es concreta la proposta de subencàrrec de tractament de dades.

5. CONDICIONS D'EXECUCIÓ: SERVEIS INCLOSOS

5.1 Obligacions bàsiques

L'adjudicatari haurà de complir les següents obligacions bàsiques:

- L'adjudicatari haurà de realitzar reunions periòdiques amb el Consorci AOC per tal d'exposar el compliment del servei on-site i tractar els possibles problemes o millores del servei.
- L'adjudicatari haurà de realitzar la formació dels tècnics designats, en tots aquells aspectes que el Consorci AOC cregui oportuns i que siguin de directa aplicació als serveis requerits.
- Presentació d'informes mensuals de presentació del servei d'acord amb els indicadors que el Consorci AOC consideri apropiats.
- Elaboració de la documentació tècnica.
- Elaboració dels manuals i altra documentació destinada a la formació dels usuaris.

5.2 Acords de nivell del servei

S'haurà de complir els requisits de l'acord de nivell de servei de l'AOC definit a les condicions generals de servei del Consorci AOC.

L'acord de nivell de servei es regularà d'acord als següents criteris.

5.2.1 Definicions de les tipologies d'incidències

Nivell	Descripció
Bloquejant	Una incidència es catalogarà amb criticitat bloquejant si impedeix la utilització total del servei a tots els usuaris d'aquest.
Alta	Una incidència es catalogarà amb criticitat alta si impedeix la utilització d'una part concreta del servei, a tots o alguns usuaris, i l'afectació pel negoci és elevada.
Mitja	Una incidència es catalogarà amb criticitat mitja si impedeix la utilització d'una funcionalitat concreta d'algun dels serveis a tots o alguns usuaris externs a la plataforma i l'afectació pel negoci és relativament baixa.
Baixa	Una incidència es catalogarà amb criticitat baixa si no impedeix la utilització ni parcial ni total d'algun dels serveis a cap dels usuaris.

5.2.2 Temps de resposta i de resolució

El temps de resposta i de resolució s'estableix segons el tipus d'incidència:

- Temps de resposta.
  Es defineix com a temps de resposta el temps que transcorre des de que la incidència es comunicada, i l'usuari rep el tiquet de la seva incidència. El temps de resposta es compta sobre l'horari de suport de recepció d'incidències.
- Temps de resolució.
  Es defineix el temps de resolució d'una incidència com el nombre d'hores que transcorren des de que l'usuari rep el tiquet de la incidència fins el moment en que la incidència està solucionada. En el càlcul del temps de resolució d'una incidència no es té en compte els possibles increments de temps provocats per la intervenció inevitable de tercers en el procés de resolució (per exemple, suport d'Oracle, intervenció d'altres organismes, etc...).
- Horari garantit segons les Condicions Generals de Servei de l'AOC
  Període de temps en que es disposa de suport tècnic especialitzat en la resolució d'incidències tècniques dels serveis del Consorci AOC.
    - Tot l'any: de dilluns a divendres 8h a 15h
    - Excepcions: dies festius de l'Estat i de Catalunya.

El temps màxim permès per la resposta i resolució d'una incidència dependrà del nivell de criticitat de la incidència. En la següent taula es mostren els temps màxims permesos per la resolució d'una incidència en funció del nivell de criticitat:

Criticitat Incidència	Temps de resposta (hores)	Temps de resolució (hores)	Horari	% de resolució dins del temps compromès
0 Bloquejant	0,5	2	horari garantit	95 %
1 Alta	1	16	horari garantit	95 %
2 Mitja	1	40	horari garantit	95 %
3 Baixa	1	64	horari garantit	95 %

Pel càlcul del temps de resolució d'una incidència s'exclouran els possibles increments de temps provocats per la intervenció inevitable en el procés de resolució per part de tercers.

6. MODEL DE RELACIÓ

6.1 Model de relació

Com a mínim, però, caldrà que s'estableixi els següents nivells d'interlocució:

- Reunions de direcció amb les següents característiques:
    - Interlocutors: cap de projecte i/o responsable del servei per part del licitador. Gestor del servei per part del Consorci AOC.

- Periodicitat: 1 mes
- Objectiu: fer el seguiment del contracte, analitzant diversos aspectes: productivitat, control d'hores, temes de facturació, seguiment de fites (a alt nivell), etc.
- Lliurables: actes de les reunions, informes executius, informes amb control d'hores (fetes i pendents) etc.

- Reunions de seguiment amb les següents característiques:
  - Interlocutors: les persones assignades pel licitador per dur a terme el servei. Per part del Consorci AOC serà el cap de projecte/servei o algun dels tècnics assignats al projecte.
  - Objectiu: seguiment del compliment de l'ANS, rendiment de la plataforma i incidències més destacables.
  - Lliurables:
    - Informe resum de les actuacions ja resoltes i hores realitzades.
    - Informe de situació de les actuacions en curs i hores realitzades.
    - Informe resum de les actuacions pendents i hores estimades.
    - Planificació de les actuacions a realitzar.
    - Escandall d'hores total realitzades en el mes.
    - Informe de les incidències obertes, resoltes, temps de resolució, etc.

6.2 Devolució del servei

L'adjudicatari haurà d'assumir sense cost per al Consorci AOC el pla de transició per fer-se càrrec del servei. Al final del servei l'adjudicatari haurà de planificar i executar el pla de devolució del servei en cas de canvi de proveïdor. El cost del pla de devolució del servei està inclòs en el pressupost del contracte.

L'adjudicatari haurà de fer una eliminació segura de tota la informació del servei una vegada aquest hagi sigut transferit.

6.3 Gestió del servei amb JIRA i Teams

La comunicació, gestió de les tasques, incidències i propostes de millora es realitzarà mitjançant l'eina JIRA i/o Teams del Consoci AOC.

6.4 Lliurables i criteris de selecció

Els lliurables i els criteris de selecció estan definit en el quadre de característiques de la present licitació.

Elena Torres

Subdirecció d’Estratègia i Innovació del Consorci AOC

ANNEX I. MESURES DE SEGURETAT DE NIVELL BAIX

Naturalesa	Grup	Mesura	Nivell	Descripció Nivell
Mesures d'Organització	Normativa, procediments i estàndards de protecció de dades	Normativa	Bàsic	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	Bàsic	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.
		Procediments d'autorització	Bàsic	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.
	Coneixement de la normativa, procediments i estàndards de protecció de dades	Deures i obligacions del personal	Bàsic	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	Bàsic	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.
Mesures de Gestió	Protecció de dades en el disseny i per defecte	Arquitectura de seguretat	Bàsic	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.

		Desenvolupament segur	Bàsic	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.
		Proves	Bàsic	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.
	Gestió d'accessos dels usuaris	Requisits d'accés i segregació de funcions	Bàsic	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.

		Identificació i autenticació	Bàsic	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.

		Gestió de drets d'accés dels usuaris	Bàsic	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	Bàsic	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.

	Gestió de Serveis Externs	Contractació i acords de nivell de servei	Bàsic	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.
Mesures de Protecció	Protecció de les instal·lacions i infraestructures	Condicionament dels locals	Bàsic	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	Bàsic	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	Bàsic	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.
	Monitorització de l'activitat i incidències	Controls d'auditoria dels sistemes de la informació	Bàsic	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.

		Registre i protecció de l'activitat dels usuaris	Bàsic	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.
		Gestió d'incidents i sistema de notificacions d'incidents	Bàsic	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.
	Protecció d'actius	Inventari d'actius	Bàsic	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	Bàsic	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	Bàsic	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	Bàsic	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	Bàsic	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.
		Devolució d'actius	Bàsic	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 de la informació	Protecció del lloc de treball	Bàsic	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.
		Limitació del tractament de dades personals	Bàsic	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	Bàsic	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.
	Protecció de la informació en tractaments no automatitzats	Control d'accés a la documentació	Bàsic	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.

		Custòdia, emmagatzematge i destrucció	Bàsic	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.
		Còpia i reproducció de documents	Bàsic	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.
		Trasllat de documentació	Bàsic	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.

		Criteris d'arxiu	Bàsic	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	Bàsic	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.
		Procediments - paper	Bàsic	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.