

**CLASSIFICACIÓ**  
**INTERN**  
**GENERALITAT DE CATALUNYA**


**AQUEST FULL NO HA DE SEPARAR-SE DEL DOCUMENT  
QUE L'ACOMPANYA**

**INFORMACIÓ IMPORTANT DEL DOCUMENT**

**Si vostè és usuari d'aquesta informació:**

- ✓ El contingut adjunt mai s'hauria de conèixer fora de l'àmbit d'actuació de la Generalitat de Catalunya i els seus proveïdors.
- ✓ El document ha d'estar custodiat en un recinte tancat.
- ✓ En cas que l'origen de l'enviament sigui una bústia genèrica, cal indicar sempre el nom de l'emissor.
- ✓ L'enviament d'aquesta informació per correu electrònic cal fer-la, sempre que sigui possible, de forma xifrada.
- ✓ L'enviament per correu postal es farà en sobre tancat, sense etiquetes externes que indiquin el nivell de classificació, i mitjançant serveis de missatgeria reconeguts per l'entitat emissora.
- ✓ S'ha de garantir que la informació adjunta estigui fora de l'abast de tercers no autoritzats.
- ✓ En el cas de transmissió de la informació a través de converses (presencials, telefòniques, videoconferències, etc.), s'ha d'incrementar el nivell de discreció per evitar que personal no usuari de la informació escolti les converses.
- ✓ En la divulgació d'aquesta informació se n'ha de garantir la integritat per evitar la modificació per part d'un tercer no autoritzat.
- ✓ En l'emmagatzematge d'aquesta informació, se n'ha de garantir que la informació queda fóra de l'abast de tercers no autoritzats.
- ✓ L'accés a aquesta informació s'ha de limitar a personal autoritzat, establint les mesures de protecció necessàries per garantir-ho (tant en format paper com en format electrònic).
- ✓ S'ha d'evitar l'exposició accidental o no intencionada de la informació a persones no usuàries de la informació.
- ✓ Els documents impresos s'han de recollir al moment, i no s'han de deixar ni oblidar a la safata de la impressora.
- ✓ En cas de ser necessària la destrucció de la informació, cal utilitzar un procediment que en garanteixi una eliminació efectiva. Si el format és paper, es recomana utilitzar destructora que impedeixi la seva recuperació o lectura. Si es tracta d'un format digital, caldrà executar un esborrat lògic estàndard.

intern



# **Marc de Ciberseguretat per a la Protecció de Dades (MCPD): Mesures de seguretat**





AGÈNCIA DE  
**CIBERSEGURETAT  
DE CATALUNYA**



**Generalitat  
de Catalunya**




El contingut d'aquesta guia és titularitat de l'Agència de Ciberseguretat de Catalunya i la resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà a través de la inclusió de la menció següent:



Llicència Creative Commons:

**Reconeixement-NoComercial-SenseObraDerivada 4.0**

**Sou lliure de copiar, distribuir i comunicar públicament l'obra, amb les següents condicions:**

-  **Reconeixement.** S'ha de reconèixer l'autoria de l'obra de la manera especificada per l'autor o el llicenciador (en tot cas, no de manera que suggereixi que gaudeix del suport o que dóna suport a la seva obra).
-  **No comercial.** No es pot emprar aquesta obra per a finalitats comercials o promocionals.
-  **Sense obres derivades.** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Quan reutilitzeu o distribuiu l'obra, heu de deixar ben clar els termes de la llicència de l'obra. Qualsevol de les condicions d'aquesta llicència podrà ser modificada si disposeu de permisos del titular dels drets.

**Podeu trobar el text legal de la llicència a:** <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.ca>

En l'exercici dels drets derivats d'aquesta llicència s'hauran de tenir en compte les possibles limitacions establertes pel nivell de classificació establert per l'Agència de Ciberseguretat de Catalunya en aquest document per tal de garantir la seguretat de la informació.



AGÈNCIA DE  
**CIBERSEGURETAT**  
DE CATALUNYA



**Generalitat**  
de Catalunya

## Fitxa del document

<b>Títol</b>	Marc de Ciberseguretat per a la Protecció de Dades (MCPD): Mesures de seguretat
<b>Fitxer físic</b>	<i>Marc de Ciberseguretat per a la Protecció de Dades_Mesures de seguretat 2.0.pdf</i>

<b>Versió</b>	<b>Redactat / Revisat per</b>	<b>Aprovat per</b>	<b>Data aprovació</b>	<b>Data publicació</b>
1.0	Àrea de Compliment Normatiu	Comitè de Direcció del CESICAT	23/07/2018	27/07/2018

<b>Registre de canvis</b>		
<b>Versió</b>	<b>Data de modificació</b>	<b>Motiu del canvi</b>
1.0	23/07/2018	Versió Inicial
1.1	21/11/2018	Correccions ortogràfiques
1.2	5/03/2019	Correccions ortogràfiques, correcció punt C.2, apartat 4.3, pàg. 11 i actualització de documents per correccions ortogràfiques (apartats 7.1, 7.2 i 7.3, pàg. 23)
1.3	14/10/2019	Correcció dels punts B.2.2, pàg. 10 i G.9, pàg.16
2.0	3/06/2021	Separació del MCPD en dos documents diferents, un que incorpora els criteris de risc i un que incorpora el catàleg de mesures de seguretat. Correcció ortogràfica títol de la mesura MP.PI.31 (apartat 4.4).

Propietari del document: Agència de Ciberseguretat de Catalunya
Nivell de classificació: Intern

# ÍNDIX

<b>01 INTRODUCCIÓ I ANTECEDENTS.....</b>	<b>1</b>
<b>02 OBJECTIUS I ABAST.....</b>	<b>3</b>
<b>03 MARCS DE REFERÈNCIA.....</b>	<b>4</b>
<b>04 MESURES DE CIBERSEGURETAT .....</b>	<b>6</b>
4.1 MESURES DE CIBERSEGURETAT PEL NIVELL DE RISC BÀSIC.....	7
4.2 MESURES DE CIBERSEGURETAT PEL NIVELL DE RISC MITJÀ .....	7
4.3 MESURES DE CIBERSEGURETAT PEL NIVELL DE RISC ALT .....	7
4.4 DETALL DE LES MESURES DE CIBERSEGURETAT .....	8



## 01 INTRODUCCIÓ I ANTECEDENTS

El 14 d'abril de 2016 el Parlament Europeu va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament General de Protecció de Dades, en endavant RGPD).

Aquesta nova regulació que, per primera vegada es va fer a través d'un reglament europeu, va comportar canvis significatius en el model de protecció de dades de caràcter personal a Catalunya, tant des del punt de vista dels drets de les persones com de les obligacions de les persones i entitats que tracten dades de caràcter personal.

La Generalitat de Catalunya i el seu sector públic, com a entitats implicades en el tractament de dades de caràcter personal en l'àmbit territorial de Catalunya, resten subjectes al compliment del RGPD, essent aquest plenament aplicable des del 25 de maig de 2018.

Posteriorment, en data 5 de desembre de 2018, es va aprovar la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals (en endavant, LOPDGDD), que completava el que disposava el RGPD.

Una de les prescripcions més rellevants que introdueix el RGPD és la necessitat, per part de l'entitat implicada en el tractament (ja sigui en el seu rol de responsable o encarregat del tractament), de definir un conjunt de mesures organitzatives i tècniques per garantir un nivell de seguretat adequat al risc, tal i com es disposa a l'article 32.1 RGPD.

Per tal de donar compliment a aquesta obligació en l'àmbit de la Generalitat de Catalunya i el seu sector públic, l'Agència de Ciberseguretat de Catalunya (en endavant, Agència), en exercici de les funcions previstes a la Llei 15/2017, de 25 de juliol, de l'Agència de Ciberseguretat de Catalunya i, especialment la relativa a impulsar i crear un marc de directrius i normes tècniques de seguretat de compliment obligatori per a l'Administració de la Generalitat i per als organismes i entitats vinculats o dependents, per tal de garantir una protecció eficaç, en particular davant el cibercrim i els ciberatacs, defineix, en el present document, el Marc de Ciberseguretat per a la Protecció de Dades (en endavant, MCPD).

El MCPD, segons estableix l'article 35 del Decret 76/2020, de 4 d'agost, d'Administració digital, és un dels instruments mínims per l'aplicació del model de ciberseguretat de la Generalitat de Catalunya.

Així doncs, el MCPD, per una banda, formalitza, en el present document, la definició d'un conjunt de mesures de ciberseguretat organitzatives i tècniques, dirigides als sistemes i processos, que suporten les activitats de tractament de la Generalitat de Catalunya i el seu sector públic i, per altra banda, defineix i recull, en un document diferenciat, la metodologia que s'emprarà per a la classificació del nivell de risc de les dites activitats de tractament.

Detallant el contingut de caire més substantiu del present document, es tracten els següents aspectes:

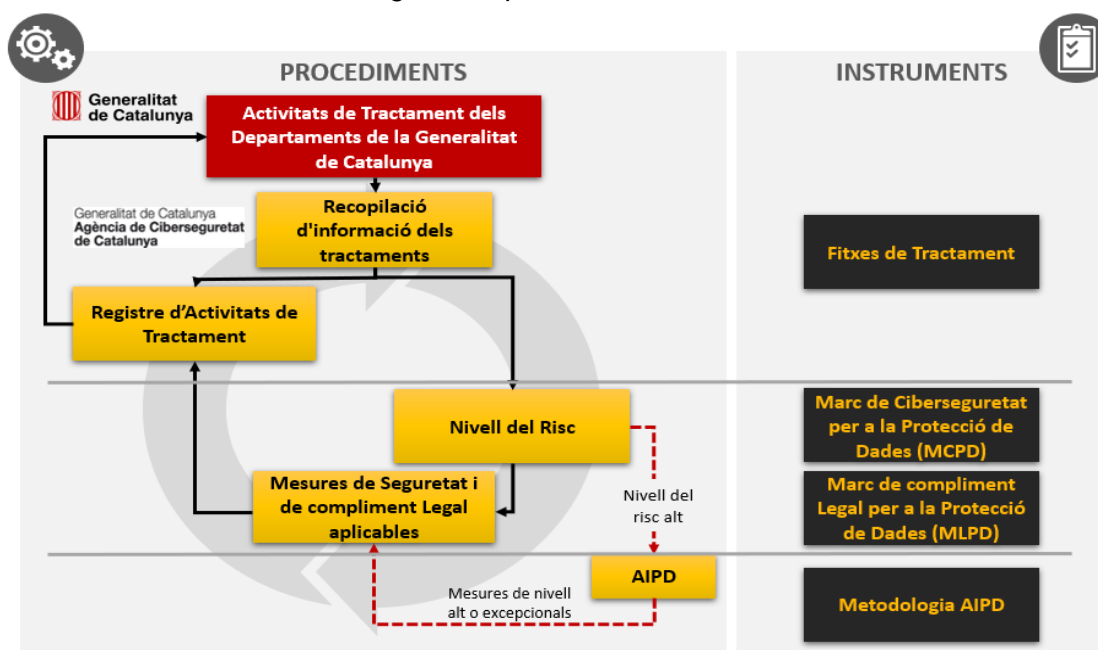
- En el punt 2. *Objectius i abast*, es defineixen les finalitats perseguides pel document i el seu àmbit d'aplicació.
- En el punt 3. *Marcs de referència*, es presenten els Marcs de referència que han servit de base per establir les mesures de ciberseguretat.
- En el punt 4. *Mesures de ciberseguretat* s'estableixen un conjunt de mesures de ciberseguretat, diferenciant-les per blocs, segons el nivell de risc obtingut per a cada activitat de tractament aplicable, en virtut dels criteris establerts al document MCPD-Criteris de risc.

## 02 OBJECTIUS I ABAST

L'objectiu d'aquest document és, un cop analitzat i classificat el nivell de risc dels tractaments, servir com a eina per a definir les mesures de ciberseguretat aplicables als esmentats tractaments. Més concretament, a través de l'anàlisi del nivell de risc i tenint en compte el model de ciberseguretat de la Generalitat de Catalunya, des de l'Agència es defineix un llistat de **mesures d'organització, de gestió i tècniques** (d'acord amb l'article 32.1 RGPD i l'article 28.1 LOPDGGD) que configuren un nivell de seguretat adequat al risc d'acord amb la normativa aplicable.

Aquest document es complementa amb la primera part del MCPD, que té com objectiu oferir una metodologia que serveixi per analitzar de forma homogènia i objectiva el **nivell de risc de les activitats de tractament de dades personals** que es duen a terme en l'àmbit d'actuació de la Generalitat de Catalunya i el seu sector públic. Aquesta anàlisi s'aplica a les activitats de tractament identificades mitjançant la Fitxa de Tractament<sup>1</sup>, instrument que l'Agència ha posat a disposició de la Generalitat de Catalunya i del seu sector públic.

A la següent *Il·lustració 1 – Diagrama de procediments i lliurables* es mostra el diagrama de processos i documents rellevants dins del model de gestió de la ciberseguretat per a la protecció de dades personals i hi encaixa el present document, a fi de concretar-ne l'abast i funció. El MCPD descriu la segona capa on es defineix la classificació del nivell de risc de les activitats de tractament analitzades i les mesures de ciberseguretat aplicables.



*Il·lustració 1 – Diagrama de procediments i instruments*

<sup>1</sup> Agència de Ciberseguretat de Catalunya. Fitxa de Tractament. Febrer de 2021.



## 03 MARCS DE REFERÈNCIA

L'article 32 RGPD estableix que "tenint en compte l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques, cal que el responsable i l'encarregat del tractament apliquin les mesures tècniques i organitzatives adequades per garantir un nivell de seguretat adequat al risc". Per tal de definir aquestes mesures de ciberseguretat s'han utilitzat diferents normes i marcs de referència.

Com a base d'aquesta definició de les mesures de ciberseguretat s'ha utilitzat el que es preveu tant en el RGPD com en l'Esquema Nacional de Seguretat (en endavant, ENS), en línia amb el previst en la Disposició Addicional Primera de la LOPDGDD.

En el disseny d'aquest catàleg de mesures s'ha tingut en compte el model de ciberseguretat de la Generalitat, que inclou en el Marc Normatiu de la Seguretat de la Informació de la Generalitat de Catalunya (Marc Normatiu) un seguit de directrius i normes tècniques que incorporen mesures de ciberseguretat específiques per a la protecció dels sistemes i plataformes de natura transversal. En aquest sentit, el MCPD compta amb aquests altres estàndards del Marc Normatiu per tal de proporcionar una cobertura completa de protecció.

A més, en la confecció del catàleg de mesures, a més de tenir en compte el Marc Normatiu, s'han consultat les mesures d'aplicació derivades de la sèrie de normes que conté la ISO27000 – *Sistemes de Gestió de la Seguretat de la Informació*, concretament en les seves parts ISO27001 – *Certificació de Sistemes de Gestió de la Seguretat de la Informació*<sup>2</sup> i ISO 27002 – *Codi de pràctiques pels controls de Seguretat de la Informació*<sup>3</sup>, així com la norma ISO/IEC 29100 *Information Technology-Security techniques-Privacy framework*<sup>4</sup> i les guies establertes pel *National Institute of Standards and Technology* (en endavant, NIST), concretament el seu estàndard 800-53 – *Controls de Seguretat i Privacitat per els sistemes d'informació i organitzacions*<sup>5</sup>.

El Marc de Ciberseguretat per a la Protecció de Dades integra la visió unificada dels marcs de referència tal i com representa la *Il·lustració 4 - Marcs de Referència*.



<sup>2</sup> UNE-ISO/IEC 27001:2014 - Certificació de Sistemes de Gestió de la Seguretat de la Informació.

<sup>3</sup> UNE-ISO/IEC 27002:2013 - Codi de pràctiques pels controls de Seguretat de la Informació.

<sup>4</sup> UNE-ISO/IEC 29100:2011 – Marc de Privacitat.

<sup>5</sup> NIST 800-53. Revisió 5. – Controls de Seguretat i Privacitat per els sistemes d'informació i organitzacions.

*Il·lustració 4 - Marcs de Referència*

Seguidament es detallen cadascun dels marcs de referència utilitzats per la definició de polítiques, procediments i processos de seguretat dels tractaments de dades:

- ❖ **RGPD:** Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, i que deroga la Directiva 95/46/CE.
- ❖ **LOPDGDD:** Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.
- ❖ **Marc normatiu de la Seguretat de la Informació de la Generalitat de Catalunya:** Està conformat per un conjunt d'estàndards que configuren una sèrie de controls per tal d'assegurar la seguretat dels sistemes d'informació específicament de la Generalitat de Catalunya.
- ❖ **ENS:** Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. Més concretament a la Guia de Seguretat de les TIC CCN-STIC 825<sup>6</sup> es considera la relació de l'ENS amb les normes ISO/IEC 27001 i ISO/IEC 27002 publicades en 2005 i revisades el 2013.
- ❖ La norma **ISO/IEC 27001** és una norma internacional, de gestió, de compliment voluntari i certificable que defineix el sistema de gestió de la seguretat del sistema d'informació. D'altra banda, la norma **ISO/IEC 27002** recull un conjunt de punts de control que poden o han de tenir-se en consideració dins del sistema de gestió en qüestió.
- ❖ La norma **ISO/IEC 29100** *Information Technology-Security techniques-Privacy framework*, que estableix un marc de referència per la protecció de les dades personals tractades mitjançant sistemes d'informació.
- ❖ L'estàndard facilitat pel *National Institute of Standards and Technology* (NIST), concretament la publicació 800-53 que forma part de la sèrie NIST 800 que integra el conjunt de documents que descriuen les polítiques, procediments i guies de la seguretat informàtica del govern federal dels Estats Units. Més concretament, **NIST 800-53** proveeix un marc de gestió del risc que condueix a la selecció de controls de seguretat pels sistemes d'informació.

---

<sup>6</sup> Esquema Nacional de Seguridad Certificaciones 27001. Noviembre 2013. Guía de Seguridad de las TIC CCN-STIC 825.

## 04 MESURES DE CIBERSEGURETAT

Al contrari que la legislació anterior al RGPD, que establia un catàleg de mesures de ciberseguretat que s'havien d'aplicar en virtut de la naturalesa i les finalitats de les dades, el RGPD obliga a realitzar una valoració dels riscos dels tractaments i, en virtut de la mateixa, mitjançant un enfoc basat en la proporcionalitat, adoptar les mesures de ciberseguretat adients.

Amb l'obtenció del nivell de risc i en base als marcs de referència identificats, a continuació es mostra el llistat de mesures de ciberseguretat que s'han definit. Aquestes mesures serviran per extreure un pla d'acció dirigit a les activitats que tractin dades de caràcter personal per complir amb el RGPD.

Aquestes mesures de ciberseguretat es classifiquen, segons el seu àmbit d'aplicació, en tres tipus: **mesures d'organització, de gestió i de protecció**, tal i com mostra la *Il·lustració 5 – Tipologia de mesures*.



Il·lustració 5 - Tipologia de mesures

Com ja s'ha mencionat amb anterioritat, un cop obtingut el nivell de risc s'assignarà un conjunt de mesures adequat a cada nivell de risc (bàsic, mitjà o alt) que definirà un pla d'acció per a cada activitat de tractament en el que es detallarà les mesures de ciberseguretat a implementar. Les mesures seran acumulatives, de manera que si el nivell és mitjà, s'aplicaran les mesures de nivell bàsic i mitjà i si el nivell és alt, s'aplicaran les mesures de nivell bàsic, mitjà i alt.

Pel que fa a les **mesures de ciberseguretat pel nivell de risc bàsic i mitjà**, seran assignades segons el mateix nivell de risc identificat directament a través de l'anàlisi de les Fitxes de Tractament.

Pel que fa a les **mesures de ciberseguretat pel nivell de risc alt**, es realitzarà en primera instància una AIPD. Segons el resultat d'aquesta, s'assignaran mesures de nivell alt o mesures addicionals, que s'hauran de valorar *ad hoc*.

A continuació s'adjunta el detall de les mesures de ciberseguretat per nivell.

#### 4.1 Mesures de ciberseguretat pel nivell de risc bàsic

*El document adjunt inclou la descripció de cadascuna de les mesures de ciberseguretat de nivell bàsic.*



MCPD\_Mesures\_Nive  
IIBasic\_v1.2.xlsx

#### 4.2 Mesures de ciberseguretat pel nivell de risc mitjà

*El document adjunt inclou la descripció de cadascuna de les mesures de ciberseguretat de nivell mitjà.*



MCPD\_Mesures\_Nive  
IIMitja\_v1.2.xlsx

#### 4.3 Mesures de ciberseguretat pel nivell de risc alt

*El document adjunt inclou la descripció de cadascuna de les mesures de ciberseguretat de nivell alt.*



MCPD\_Mesures\_Nive  
IIAlt\_v1.2.xlsx

#### 4.4 Detall de les mesures de ciberseguretat

A continuació s'estableix el detall complet de les mesures de ciberseguretat per blocs i nivells:

Naturalesa	[MO] - Mesures d'Organització
Grup	[MO.NO] - Normativa, procediments i estàndards de protecció de dades
Mesura	<b>[MO.NO.01] - Normativa</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. La Normativa de protecció de dades ha de plasmar de forma clara i precisa, almenys, el següent:</p> <p>a) Organització de protecció de dades:</p> <ul style="list-style-type: none"> <li>- Designació del Delegat de Protecció de Dades (DPD) dels tractaments automatitzats i no automatitzats.</li> <li>- 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.</li> <li>- Designació del Responsable de ciberseguretat i compliment de protecció de dades.</li> <li>- Definició dels rols i funcions definint per a cadascun els deures i responsabilitats.</li> </ul> <p>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.</p> <p>c) Model de relació amb l'autoritat de control.</p> <p>d) Registre d'Activitats de Tractament que haurà de contenir com a mínim els següents camps:</p> <ul style="list-style-type: none"> <li>- Nom i dades de contacte del DPD, del Responsable del Tractament i, si s'escau, del corresponsable i del representant del responsable.</li> <li>- Activitats i finalitats dels tractaments.</li> <li>- Descripció de les categories de dades i dels interessats.</li> <li>- Categories dels destinataris a qui se li han comunicat o comunicaran les dades, inclosos els destinataris en tercers països o organitzacions internacionals.</li> <li>- Transferències internacionals de dades.</li> <li>- Quan sigui possible, els terminis previstos per a la supressió de les diferents categories de dades.</li> </ul>

	<p>- Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat.</p> <p>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:</p> <ul style="list-style-type: none"> <li>- Nom i dades de contacte del encarregat i de cada responsable per compte del que actui i, si s'escau, del representant del responsable o del encarregat i del DPD.</li> <li>- Categories de tractaments efectuats per compte de cada responsable.</li> <li>- Transferències internacionals de dades.</li> </ul> <p>- Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat.</p> <p>f) Identificació de les Activitats de Tractament i sistemes d'informació associats.</p> <p>g) Definició dels nivells de risc de les Activitats de Tractament i els criteris per la classificació.</p> <p>h) Metodologia d'Avaluació d'Impacte relativa a la Protecció de Dades (AIPD).</p> <p>i) Identificació de les mesures de ciberseguretat associades als diferents nivells de risc.</p> <p>2. La normativa referida en aquest apartat haurà de mantenir-se en tot moment actualitzada i serà revisada sempre que es produeixin canvis rellevants.</p> <p>3. Qualsevol incompliment o excepció de la normativa haurà de ser correctament documentat.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>4. S'haurà de disposar de la documentació d'un sistema de gestió de seguretat de la informació aprovada i actualitzada.</p>
Naturalesa	[MO] - Mesures d'Organització
Grup	[MO.NO] - Normativa, procediments i estàndards de protecció de dades
Mesura	[MO.NO.02] - Procediments
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>a) Control d'accés lògic (gestió d'usuaris). Ha d'incloure el control d'accés a les dades que tenen limitat el tractament.</li> <li>b) Identificació i autenticació.</li> <li>c) Gestió de suports.</li> <li>d) Còpies de seguretat i restauració de dades.</li> </ul>

	<p>e) Control d'accés físic.</p> <p>f) Tractament de fitxers temporals.</p> <p>g) Eliminació segura d'informació en la reutilització o destrucció de suports i sistemes.</p> <p>h) Devolució d'actius.</p> <p>i) Registre d'accessos.</p> <p>j) Gestió d'excepcions.</p> <p>k) Treball fora dels locals del responsable de les Activitats de Tractament o encarregats dels tractaments.</p> <p>l) Notificació, registre i gestió d'incidències.</p> <p>m) Notificació de vulneracions de seguretat.</p> <p>2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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:</p> <p>a) Pseudonimització.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>4. S'ha de disposar, com a mínim, dels següents documents que detallin de forma clara i precisa com portar a terme els tractaments automatitzats:</p> <p>a) Transmissió de dades per xarxes públiques.</p> <p>b) Gestió i distribució de suports.</p>
Naturalesa	[MO] - Mesures d'Organització
Grup	[MO.NO] - Normativa, procediments i estàndards de protecció de dades
Mesura	<b>[MO.NO.03] - Procediments d'autorització</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes:</p> <p>a) Ús de dispositius mòbils (ordinadors portàtils, dispositius mòbils intel·ligents, tauletes, agendes electròniques, etc.).</p> <p>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.)).</p> <p>c) Sortida de dispositius mòbils i suports.</p>

	<p>d) Tractament fora dels locals del Responsable del Tractament o Encarregat del Tractament.</p> <p>e) Accés remot.</p> <p>f) Execució dels procediments de recuperació de dades.</p> <p>g) Entrada en producció i manteniment d'equips i aplicacions.</p> <p>2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>3. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes:</p> <p>a) Execució del Pla de Continuitat i les proves periòdiques.</p>
Naturalesa	[MO] - Mesures d'Organització
Grup	[MO.CN] - Coneixement de la normativa, procediments i estàndards de protecció de dades
Mesura	<b>[MO.CN.04] - Deures i obligacions del personal</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. S'ha d'informar al personal de:</p> <p>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.</p> <p>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.</p> <p>c) Les mesures disciplinàries en cas d'incompliment.</p>
Naturalesa	[MO] - Mesures d'Organització
Grup	[MO.CN] - Coneixement de la normativa, procediments i estàndards de protecció de dades
Mesura	<b>[MO.CN.05] - Formació i conscienciació</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <p>a) La normativa, procediments i estàndards de seguretat relativa al bon ús dels sistemes i els tractaments en paper.</p> <p>b) La detecció i reacció a incidents de seguretat, activitats o comportaments sospitosos.</p>



	<p>c) El procediment de notificació d'incidents i vulneracions de seguretat.</p> <p>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.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.PD] - Protecció de dades en el disseny i per defecte
Mesura	<b>[MG.PD.06] - Arquitectura de seguretat</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>S'han de dissenyar i configurar els sistemes i xarxes aplicant la regla de mínima funcionalitat i la seguretat per defecte.</li> <li>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.</li> <li>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: <ol style="list-style-type: none"> <li>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.</li> <li>la retirada de comptes i contrasenyes per defecte.</li> <li>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.</li> <li>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.</li> </ol> </li> <li>S'ha de mantenir documentació tant del disseny d'arquitectura com de la configuració dels equips.</li> <li>De manera prèvia a l'entrada en producció s'ha de realitzar un anàlisi de vulnerabilitats.</li> <li>S'ha de demanar autorització relativa a l'entrada en producció i manteniment d'equips i aplicacions.</li> </ol> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>S'ha de formalitzar i documentar el disseny de l'arquitectura de seguretat i la configuració dels equips.</li> <li>La descripció del disseny i configuració ha de contemplar: <ol style="list-style-type: none"> <li>Instal·lacions: nombre, ubicació, àrees existents i detall dels punts d'accés.</li> <li>Sistemes: inventari dels sistemes d'informació que, com a mínim, contingui: <ul style="list-style-type: none"> <li>Els actius dels sistemes (servidor de correu, robot de backup...).</li> </ul> </li> </ol> </li> </ol>

	<ul style="list-style-type: none"> <li>- Les xarxes existents, així com els elements de connexió a l'exterior (p.ex. la xarxa local està separada d'Internet mitjançant un tallafocs).</li> <li>- Els punts d'accés als sistemes (llocs de treball, consols d'administració, web de la intranet, etc.).</li> </ul> <p>c) Esquema de línies de defensa:</p> <ul style="list-style-type: none"> <li>- Inventari dels sistemes de seguretat (tallafocs, DMZ, antivirus, antispam, etc.).</li> <li>- Elements d'interconnexió a altres sistemes o a altres xarxes.</li> <li>- Elements de defensa en les connexions a altres xarxes (per exemple, la connexió amb Internet es realitza a través d'un tallafocs).</li> <li>- Utilització de tecnologies diferents per prevenir vulnerabilitats que puguin perforar simultàniament diverses línies de defensa.</li> </ul> <p>d) Sistema d'identificació i autenticació d'usuaris per a cada sistema o servei:</p> <ul style="list-style-type: none"> <li>- Ús de claus concertades, contrasenyes, targetes d'identificació, biometria, o altres de naturalesa anàloga.</li> <li>- Ús de fitxers o directoris per autenticar l'usuari i determinar els seus drets d'accés.</li> </ul> <p>e) Sistema de gestió, relatiu a la planificació, l'organització i el control dels recursos relatius a la seguretat de la informació.</p> <p>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.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.PD] - Protecció de dades en el disseny i per defecte
Mesura	<b>[MG.PD.07] - Desenvolupament segur</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. S'ha d'aplicar una metodologia de desenvolupament reconeguda que: <ol style="list-style-type: none"> <li>a) Prengui en consideració els aspectes de seguretat en tot el cicle de vida.</li> <li>b) Utilitzi algoritmes, programari i biblioteques reconegudes.</li> <li>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 MP.MO.20 "Registre i protecció de l'activitat dels usuaris".</li> </ol> </li> <li>3. De manera prèvia a l'entrada en producció s'ha de realitzar: <ol style="list-style-type: none"> <li>a) Comprovació del funcionament correcte de l'aplicació.</li> </ol> </li> </ol>

	<p>b) Anàlisi de vulnerabilitats.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>4. S'ha d'aplicar una metodologia de desenvolupament reconeguda que:</p> <p>a) Permeti la inspecció del codi font.</p> <p>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).</p> <p>5. De manera prèvia a l'entrada en producció s'ha de realitzar:</p> <p>a) Proves de penetració.</p> <p>b) Anàlisi del codi font.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.PD] - Protecció de dades en el disseny i per defecte
Mesura	<b>[MG.PD.08] - Proves</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. Les proves s'han de fer en un entorn aïllat del de producció.</p> <p>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.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.GA] - Gestió d'accessos dels usuaris
Mesura	<b>[MG.GA.09] - Requisits d'accés i segregació de funcions</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. Els requisits d'accés s'han d'atènyer al que s'indica a continuació:</p> <p>a) Tot sistema d'informació ha de disposar de mecanismes d'autenticació per a validar la identitat dels usuaris que hi accedeixen.</p> <p>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.</p> <p>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'atènyer a la normativa de seguretat del sistema.</p> <p>d) Particularment, s'ha de controlar l'accés als components del sistema i als seus fitxers o registres de configuració.</p>

	<p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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 duuguin 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.</p> <p>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:</p> <p>a) Desenvolupament d'operació.</p> <p>b) Configuració i manteniment del sistema d'operació.</p> <p>c) Auditoria o supervisió de qualsevol altra funció.</p> <p>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.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.GA] - Gestió d'accessos dels usuaris
Mesura	[MG.GA.10] - Identificació i autenticació
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- De manera telemàtica, mitjançant DNI electrònic o un certificat electrònic qualificat.</li> <li>- De manera telemàtica, utilitzant altres sistemes admesos legalment per a la identificació dels ciutadans dels que prevegi la normativa aplicable.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>- "Factors de coneixement": contrasenyes o claus concertades. Han de disposar de regles bàsiques de qualitat (extensió, tipus de caràcters, etc.).</li> <li>- "Factors de possessió": components lògics (com ara certificats de programari) o dispositius físics (tokens, telèfons mòbils, dispositius).</li> </ul>

	<p>- “Factors inherents o propis de l'usuari”: elements biomètrics.</p> <p>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).</p> <p>4. La identificació dels usuaris del sistema s'ha de fer d'acord amb el que s'indica a continuació:</p> <p>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.</p> <p>b) Es poden utilitzar com a identificador únic els sistemes d'identificació que prevegi la normativa aplicable.</p> <p>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.</p> <p>d) Cada entitat (usuari o procés) que accedeix al sistema ha de disposar d'un identificador únic de manera que:</p> <ul style="list-style-type: none"> <li>- Es pot saber qui rep i quins drets d'accés rep.</li> <li>- Es pot saber qui ha fet alguna cosa i què ha fet.</li> </ul> <p>5. Les credencials s'han de gestionar de la manera següent:</p> <p>a) S'han d'activar una vegada estiguin sota el control efectiu de l'usuari.</p> <p>b) Han d'estar sota el control exclusiu de l'usuari.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>f) S'han de revisar periòdicament els identificadors i verificar si és necessari que accedeixin als sistemes d'informació.</p> <p>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.</p>
--	--

	<p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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.</p> <p>7. Les credencials utilitzades s'han d'haver obtingut després d'una registre previ:</p> <p>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.</p> <p>b) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat.</p> <p>) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat en un dispositiu de creació de signatura.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>8. Les credencials s'han de suspendre després d'un període definit de no-utilització.</p> <p>9. En el cas de l'ús d'utilització d'un factor de possessió, es requereix l'ús d'elements criptogràfics de maquinari amb la utilització d'algoritmes i paràmetres validats al Protocol d'identificació i signatura electrònica del Marc Normatiu de la Generalitat de Catalunya o bé reconeguts a la TSL (Trust-service Status List) aplicable.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.GA] - Gestió d'accessos dels usuaris
Mesura	<b>[MG.GA.11] - Gestió de drets d'accés dels usuaris</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p>2. Els drets d'accés de cada usuari s'han de limitar atenent els principis següents:</p> <p>a) Mínim privilegi. Els privilegis de cada usuari s'han de reduir al mínim estrictament necessari per complir les seves obligacions.</p> <p>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.</p> <p>3. L'assignació de drets ha de tenir en compte el següent:</p> <p>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.</p>

	<p>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.</p> <p>c) Han de definir-se els requisits per al venciment dels drets d'accés privilegiats.</p> <p>d) Els drets d'accés han d'assignar-se a un identificador d'usuari.</p> <p>e) S'han de revisar periòdicament els permisos assignats als usuaris i, verificar que es corresponen a les seves funcions.</p> <p>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.</p> <p>g) S'han d'establir i mantenir procediments per a evitar l'ús no autoritzat de l'identificador d'usuari, en especial pel que fa a aquelles credencials amb permisos d'administrador.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.GA] - Gestió d'accessos dels usuaris
Mesura	<b>[MG.GA.12] - Accés local i remot</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>2. Els accessos hauran de complir amb les següents mesures segons el nivell dels tractaments:</p> <p>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).</p> <p>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.</p>

	<p>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.</p> <p>3. S'aplicaran a les connexions en remot les mesures de ciberseguretat 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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>4. S'ha d'informar l'usuari de l'últim accés efectuat amb la seva identitat.</p> <p>5. S'ha d'establir una política específica del que es pot fer remotament, per a la qual cosa es requereix autorització positiva.</p> <p>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.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>7. L'accés ha d'estar limitat per horari, dates i lloc des d'on s'accedeix.</p> <p>8. S'han de definir els punts en què el sistema requereix una renovació de l'autenticació de l'usuari, mitjançant identificació singular, sense que n'hi hagi prou amb la sessió establerta.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.GS] - Gestió de Serveis Externs
Mesura	<b>[MG.GS.13] - Contractació i acords de nivell de servei</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. S'han de subscriure, si són d'aplicació els escenaris descrits, els següents contractes o altres actes jurídics amb els següents actors:</p> <p>a) Encarregats del Tractament. Aquests han d'establir de forma clara i concisa, com a mínim:</p> <ul style="list-style-type: none"> <li>- Objecte.</li> <li>- Durada.</li> <li>- Naturalesa i finalitat del tractament (característiques del servei prestat).</li> <li>- Tipus de dades personals.</li> <li>- Categoria dels interessats.</li> <li>- Obligacions, responsabilitats i drets del Responsable.</li> <li>- Obligacions, responsabilitats i drets de l'Encarregat segons el clausulat de l'article 28.3 RGPD.</li> </ul>



	<ul style="list-style-type: none"> <li>- Mesures tècniques i organitzatives que ofereixin unes garanties suficients d'acord amb el nivell de risc de les dades.</li> <li>- Nivells de servei (temps de resposta en cas de violacions de seguretat, resolució d'incompliments, etc.).</li> <li>- Conseqüències de l'incompliment.</li> <li>- Devolució o destrucció de les dades a la finalització de l'encàrrec.</li> </ul> <p>b) Prestadors de serveis sense accés a dades. Aquests han d'establir de forma clara i concisa, com a mínim:</p> <ul style="list-style-type: none"> <li>- Naturalesa i finalitat del servei.</li> <li>- Prohibició d'accedir a les dades personals.</li> <li>- Obligació de deure de secret respecte a les dades que el personal hagués pogut conèixer amb motiu de la prestació de servei.</li> <li>- Conseqüències de l'incompliment.</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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.</p> <p>7. Els contractes hauran de preveure la revisió de les condicions de tractament.</p> <p>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.</p>
--	---

Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.CS] - Continuitat del servei
Mesura	<b>[MG.CS.14] - Pla de continuïtat</b>
Descripció	<p><b>- Pel nivell alt:</b></p> <p>1. S'ha de desenvolupar un pla de continuïtat que estableixi les accions a executar en cas d'interrupció dels serveis prestats amb els mitjans habituals. Aquest pla ha de preveure els aspectes següents:</p> <p>a) S'han d'identificar funcions, responsabilitats i activitats a realitzar.</p> <p>b) Hi ha d'haver una previsió dels mitjans alternatius que es conjugaran per poder seguir prestant els serveis.</p> <p>c) Tots els mitjans alternatius han d'estar planificats i materialitzats en acords o contractes amb els proveïdors corresponents.</p> <p>d) Els serveis i mitjans alternatius de comunicació han de:</p> <ul style="list-style-type: none"> <li>- Tenir les mateixes garanties de seguretat que els habituals.</li> <li>- Garantir temps màxim d'entrada en funcionament segons els terminis determinats a l'anàlisi d'impacte i/o acordats en el Pla de Continuitat.</li> </ul> <p>e) Les persones afectades pel pla han de rebre formació específica relativa al seu paper en l'esmentat pla.</p> <p>f) El pla de continuïtat ha de ser part integral i harmònica dels plans de continuïtat de l'organització en altres matèries alienes a la seguretat.</p> <p>2. L'execució del Pla de Continuitat, així com qualsevol procediment de recuperació dins el mateix, haurà de ser prèviament autoritzat per la Generalitat de Catalunya.</p>
Naturalesa	[MG] - Mesures de Gestió
Grup	[MG.CS] - Continuitat del servei
Mesura	<b>[MG.CS.15] - Proves periòdiques</b>
Descripció	<p><b>- Pel nivell alt:</b></p> <p>1. S'han de fer proves periòdiques per localitzar i corregir, si s'escau, els errors o deficiències que hi puguin haver en el pla de continuïtat.</p> <p>2. L'execució del pla de proves haurà de ser prèviament aprovat per la Generalitat de Catalunya.</p>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.II] - Protecció de les instal·lacions i infraestructures
Mesura	<b>[MP.II.16] - Condicionament dels locals</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <p>a) Condicions de temperatura i humitat.</p> <p>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.</p> <p>c) Protecció contra les amenaces identificades a l'anàlisi de riscos.</p> <p>d) Protecció del cablatge contra incidents fortuïts o deliberats.</p> <p>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.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.II] - Protecció de les instal·lacions i infraestructures
Mesura	<b>[MP.II.17] - Control d'accés físic</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p>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.</p> <p>2. El registre d'accessos ha d'estar controlat per una persona autoritzada.</p>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.II] - Protecció de les instal·lacions i infraestructures
Mesura	<b>[MP.II.18] - Registre d'entrada i sortida d'equipament i suports</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. S'ha d'elaborar una llista de serveis autoritzats de transport o missatgeria a emprar.</li> <li>3. S'ha de disposar d'un procediment informal que compari les sortides amb les arribades per tal de detectar algun incident.</li> </ol> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.MO] - Monitorització de l'activitat i incidències
Mesura	<b>[MP.MO.19] - Controls d'auditoria dels sistemes de la informació</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>1. El Responsable de tractament haurà de tenir un model de compliment que permeti el seguiment, revisió i autoavaluació de les mesures de ciberseguretat aplicades als tractaments 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.</li> </ol> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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 ciberseguretat.</li> </ol>

	<p>3. Les auditories podran ser internes o externes però les persones que les portin a terme hauran de ser independents i expertes.</p> <p>4. Les auditories es realitzaran segons els criteris i estàndards establerts pel CESICAT.</p> <p>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.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.MO] - Monitorització de l'activitat i incidències
Mesura	<b>[MP.MO.20] - Registre i protecció de l'activitat dels usuaris</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. S'han de registrar les activitats dels usuaris en el sistema, de manera que:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>2. S'han d'activar els registres d'activitat en els servidors.</p> <p>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).</p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>6. S'ha de revisar formalment i s'ha de disposar d'un sistema automàtic de recol·lecció de registres i correlació d'esdeveniments. Els esdeveniments s'hauran de recollir en aquest sistema automàtic, d'acord amb el model TIC de la Generalitat de Catalunya. Aquest</p>

	sistema podrà ser transversal i/o operat per organismes competents en matèria de ciberseguretat, com el CESICAT.
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.MO] - Monitorització de l'activitat i incidències
Mesura	<b>[MP.MO.21] - Gestió d'incidents i sistema de notificacions d'incidents</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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 més, s'hauran de registrar les restauracions de còpies de seguretat, indicant la persona que realitza el procés, les dades restaurades i les dades que s'hagin hagut de gravar manualment en el procés de recuperació.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que:</p> <p>a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident.</p> <p>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.</p> <p>c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments.</p> <p>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:</p> <p>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.</p> <p>b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals.</p> <p>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.</p>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.22] - Inventari d'actius</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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: <ol style="list-style-type: none"> <li>a) El responsable.</li> <li>b) Tipus d'actiu (servidor, ordinador, router, etc.).</li> <li>c) Identificador, fabricant i model.</li> <li>d) Ubicació.</li> </ol> </li> <li>2. Els inventaris s'actualitzaran en funció dels terminis establerts a la normativa.</li> </ol>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.23] - Fitxers temporals</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Tot fitxer temporal així creat serà esborrat una vegada hagi deixat de ser necessari per la finalitat que va motivar la seva creació.</li> </ol>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.24] - Protecció d'equips</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Els equips han de disposar de protecció antivirus i antimalware.</li> <li>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</li> </ol>

	<p>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.</p> <p><b>- Addicionalment pel nivell alt:</b></p> <p>En relació amb els equips que siguin susceptibles de sortir de les instal·lacions de l'organització:</p> <p>4. S'ha de dotar el dispositiu de detectors de vulneracions que permetin saber si l'equip ha estat manipulat i activin els procediments previstos de gestió de l'incident.</p> <p>5. Les dades dels tractaments de nivell alt emmagatzemades s'han de protegir mitjançant xifratge.</p> <p>6. S'han d'establir mesures de protecció en llocs públics com filtres de confidencialitat o cadenat de seguretat.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.25] - Manteniment d'equipament</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <p>1. Les especificacions dels fabricants pel que fa a la instal·lació i manteniment dels sistemes.</p> <p>2. Un seguiment continu dels anuncis de defectes, utilitzant mecanismes, com per exemple, la subscripció de correu d'avís de defectes per part del fabricant.</p> <p>3. Un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pedaços, millores i noves versions.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.26] - Protecció dels suports d'informació</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p>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</p>



	<p>mitjançant simple inspecció, o bé mitjançant el recurs a un repositori, puguin entendre el significat.</p> <p>3. Es podrà excloure, per previsió a la normativa, l'obligació d'etiquetatge en cas de suports en que no es pugués complir per les seves característiques físiques, establint mesures alternatives per assegurar la seva identificació i localització.</p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>5. S'han de destruir de manera segura els suports d'informació, en els casos següents:</p> <p>a) Quan la naturalesa del suport no permeti un esborrat segur.</p> <p>b) Quan així ho requereixi el procediment associat al tipus d'informació continguda.</p> <p>6. S'han d'aplicar mecanismes de xifrat que garanteixin la confidencialitat i la integritat de la informació continguda en tots els suports.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PA] - Protecció d'actius
Mesura	<b>[MP.PA.27] - Devolució d'actius</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PI] - Protecció de la informació
Mesura	<b>[MP.PI.28] - Protecció del lloc de treball</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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.</p>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PI] - Protecció de la informació
Mesura	<b>[MP.PI.29] - Limitació del tractament de dades personals</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Control d'accés.</li> <li>2. Ubicació de les dades en un sistema diferent.</li> <li>3. Xifrat.</li> </ol>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PI] - Protecció de la informació
Mesura	<b>[MP.PI.30] - Còpies de Seguretat</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Aquestes còpies han de tenir el mateix nivell de seguretat que les dades originals.</li> <li>3. Les còpies de seguretat han d'incloure: <ol style="list-style-type: none"> <li>a) Informació de treball de l'organització que es refereixi a dades personals.</li> <li>b) Aplicacions en explotació, incloent-hi els sistemes operatius mitjançant les que es tractin dades personals.</li> <li>c) Claus utilitzades per preservar la confidencialitat de les dades.</li> </ol> </li> <li>4. Semestralment es verificarà la correcta definició, funcionament i aplicació dels procediments de realització de les còpies i dels procediments de recuperació.</li> <li>5. La recuperació de còpies haurà de ser autoritzada pel Responsable del tractament.</li> </ol> <p><b>- Addicionalment pel nivell alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PI] - Protecció de la informació
Mesura	<b>[MP.PI.31] – Pseudonimització</b>
Descripció	<p><b>- Pels nivells mitjà i alt:</b></p> <p>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.</p> <p>2. Les tècniques de pseudonimització han d'incloure com a mínim:</p> <p>a) Que els atributs estiguin lligats a àlies aleatoris i que no siguin suficients per identificar l'interessat a qui es refereixen.</p> <p>b) L'assignació d'àlies és tal que no es pot revertir sense esforços desproporcionats de les parts interessades.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PI] - Protecció de la informació
Mesura	<b>[MP.PI.32] - Xifrat</b>
Descripció	<p><b>- Pel nivell alt:</b></p> <p>La informació s'ha de xifrar tant durant l'emmagatzematge com durant la transmissió. Només pot estar en clar mentre se n'està fent ús.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.33] - Control d'accés a la documentació</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>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.</p>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.34] - Custòdia, emmagatzematge i destrucció</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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 impedit l'accés a qualsevol persona no autoritzada.</li> <li>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.</li> <li>4. S'ha de destruir qualsevol document que contingui dades de caràcter personal que sigui rebutjat.</li> <li>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.</li> </ol>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.35] - Còpia i reproducció de documents</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <ol style="list-style-type: none"> <li>2. S'ha de limitar únicament al personal autoritzat pel responsable del tractament la generació de còpies o la reproducció de documents.</li> </ol>

Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.36] - Trasllet de documentació</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p> <p>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.</p> <p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>3. S'han d'adoptar mesures dirigides a impedir l'accés a la informació objecte del trasllat o a la seva manipulació.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.37] - Criteris d'arxiu</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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 de 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.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.38] - Gestió d'incidents i sistema de notificacions d'incidents</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>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.</p>

	<p><b>- Addicionalment pels nivells mitjà i alt:</b></p> <p>2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que:</p> <p>a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident.</p> <p>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.</p> <p>c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments.</p> <p>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:</p> <p>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.</p> <p>b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals.</p> <p>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.</p>
Naturalesa	[MP] - Mesures de Protecció
Grup	[MP.PP] - Protecció de la informació en tractaments no automatitzats
Mesura	<b>[MP.PP.39] – Procediments per tractaments no automatitzats</b>
Descripció	<p><b>- Pels nivells bàsic, mitjà i alt:</b></p> <p>1. S'ha de disposar dels següents procediments pels tractaments no automatitzats:</p> <p>a) Treball fora dels locals del responsable de les activitats dels tractaments o encarregats dels tractaments.</p> <p>b) Notificació, registre i gestió d'incidències.</p> <p>c) Control d'accés.</p> <p>d) Criteris d'arxiu.</p> <p>e) Dispositius d'emmagatzematge.</p> <p>f) Custòdia.</p>

	<p>g) Còpia o reproducció.</p> <p>h) Trasllat.</p> <p>i) Destrucció paper.</p> <p>- <b>Addicionalment pels nivells mitjà i alt:</b></p> <p>j) Registre accés.</p> <p>- <b>Addicionalment pel nivell alt:</b></p> <p>k) Emmagatzematge.</p>
--	--



*[www.ciberseguretat.cat](http://www.ciberseguretat.cat)*

