

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): Criteris de risc





**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 la Agència de Ciberseguretat de Catalunya en aquest document per tal de garantir la seguretat de la informació.



Fitxa del document

Títol	Marc de Ciberseguretat per a la Protecció de Dades (MCPD): Criteris de risc
Fitxer físic	<i>MCPD_Criteris de risc 2.0.pdf</i>

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

Registre de canvis		
Versió	Data de modificació	Motiu del canvi
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
1.4	12/03/2021	Actualització per respondre als canvis normatius i interpretatius. Separació del MCPD en dos documents diferents, un que incorpora els criteris de risc i un que incorpora el catàleg de mesures de seguretat.
1.5	14/05/2021	Canvis de l'apartat 4.4 realitzats arran dels treballs realitzats en el marc del Grup d'Experts i Delegats de Protecció de Dades de la Generalitat de Catalunya i el seu sector públic.
2.0	3/06/2021	Generació nova versió, canvi de l'apartat 4 retirant enllaç a Fitxa de tractament i correcció errors taula 8.

Propietari del document: Agència de Ciberseguretat de Catalunya

Nivell de classificació: Intern

ÍNDIX

01 INTRODUCCIÓ I ANTECEDENTS.....	1
02 OBJECTIUS I ABAST.....	3
03 CRITERIS PER A LA CLASSIFICACIÓ DE TRACTAMENTS	4
04 ANÀLISI DE LES ACTIVITATS DE TRACTAMENT	9
4.1 INFORMACIÓ GENERAL	10
4.2 ACTIVITAT DE TRACTAMENT	10
4.3 CARACTERÍSTIQUES DE L'ACTIVITAT DE TRACTAMENT.....	11
4.4 DESCRIPCIÓ I FINALITATS DE L'ACTIVITAT DE TRACTAMENT.....	12
4.5 COL·LECTIUS D'INTERESSATS.....	13
4.6 CONTEXT DE TRACTAMENT	13
4.7 MODEL DE TRACTAMENT	14
05 DEFINICIÓ DE LA CLASSIFICACIÓ DEL NIVELL DE RISC	15

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

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

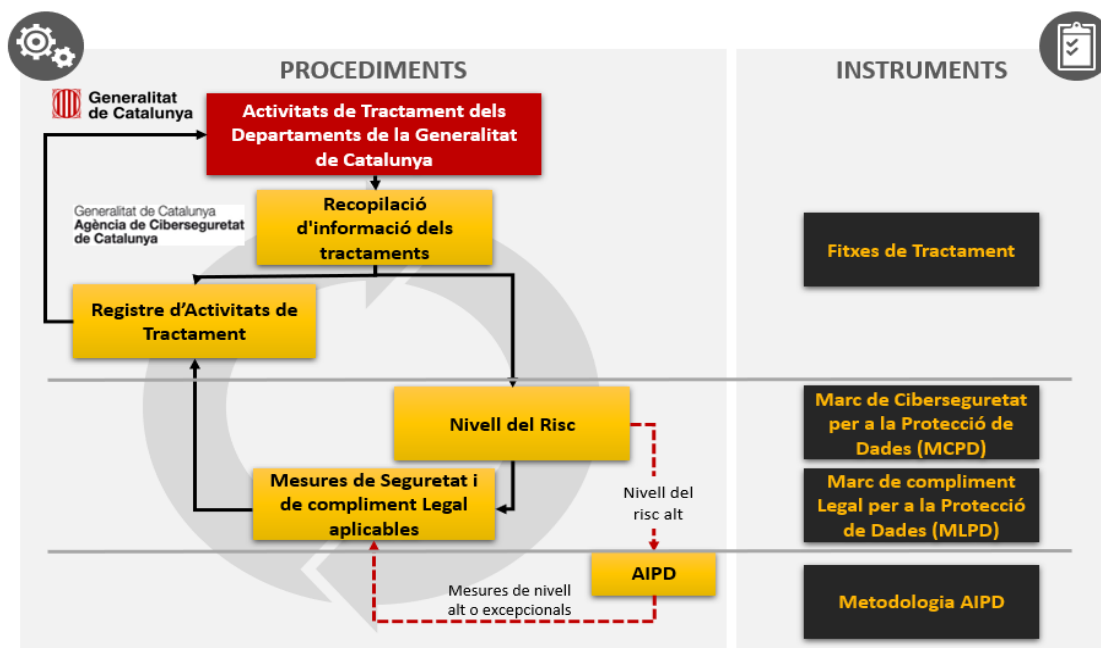
- En el punt 2. *Objectius i abast*, es defineixen les finalitats perseguides pel document i el seu àmbit d'aplicació.
- En el punt 3. *Criteris per a la Classificació de Tractaments*, es concreten les variables utilitzades per identificar els criteris de risc vinculats a les activitats de tractament.
- Al punt 4. *Anàlisi de les Activitats de Tractament* es relacionen els criteris del punt tres amb els apartats de la plantilla de la Fitxa de Tractament, que va elaborar l'Agència amb la finalitat d'agrupar i analitzar tota la informació relativa als tractaments. Aquesta relació facilita posteriorment la classificació de cadascun dels tractaments en nivells de risc.
- La classificació agregada de les activitats de tractament pel nivell de risc s'exposa en detall al punt 5. *Definició de la classificació del nivell de risc*.

02 OBJECTIUS I ABAST

L'objectiu d'aquest document, la primera part del MCPD, és 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 analitzades a través de les Fitxes de Tractament que s'han posat a disposició de la Generalitat de Catalunya i del seu sector públic per part de l'Agència.

Aquest document es complementa amb la segona part del MCPD que, té com objectiu, 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 configurin un nivell de seguretat adequat al risc d'acord amb la normativa aplicable.

A la següent *Il·lustració 1 – Diagrama de procediments i instruments* es mostra el diagrama de processos i documents rellevants dins del model de gestió de la ciberseguretat per a la protecció de dades personals, on s'encaixen els dos documents que conformen el MCPD, 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

03 CRITERIS PER A LA CLASSIFICACIÓ DE TRACTAMENTS

Com a base per avaluar de forma sistemàtica el nivell de risc resultant de les activitats de tractament, s'han de definir inicialment els criteris de risc a què poden estar exposats els tractaments de dades personals. A diferència del model anterior, on la criticitat o el nivell de seguretat que es considerava per a la protecció de dades derivava exclusivament de la naturalesa de les dades, el RGPD i la LOPDGDD defineixen determinats elements com a rellevants:

- **Naturalesa de les dades:** En funció de la tipologia de les dades o dels col·lectius d'interessats a qui pertanyen aquestes dades (p.ex. categories especials o de col·lectius vulnerables).
- **Abast del tractament:** Conjunt de dades que es processen de les persones o, fins i tot, el conjunt i volum de persones implicades en el tractament (p.ex. quan el tractament sigui de gran escala o quan la varietat de dades del tractament sigui significativament elevat); o si es realitzen transferències internacionals de dades.
- **El context del tractament:** Vinculat principalment al context del tractament de dades derivat de l'estat de la tècnica i dels mitjans de tractament. Els mitjans del tractament inclouen aspectes relatius a com es realitza aquest tractament, és a dir, els mitjans tècnics i organitzatius, les dades recollides, les operacions concretes de tractament, el termini de conservació de les dades o qui pot tenir accés a aquestes dades¹.
- **Les finalitats del tractament:** Les finalitats a què es destinin les dades processades, que reflecteixen les noves tendències en els tractaments que afavoreix la tecnologia, com les avaluacions de perfils o les anàlisis predictives.

Així mateix, en els anteriors elements de risc s'integrarien els factors de risc llistats en l'article 28.2 de la LOPDGDD, que s'hauran de tenir en consideració en l'adopció de mesures tècniques i organitzatives apropiades, així com a l'hora de valorar si escau fer una Avaluació d'Impacte relativa a la Protecció de Dades (en endavant, AIPD) i consulta prèvia.

Per tal de concretar els elements de risc dins de les esmentades categories s'ha avaluat la normativa², la interpretació dels criteris de risc que es van incloure en el Document de Treball del Grup de l'Article 29 WP 248³, on es fixaven els criteris per mesurar si el tractament pot comportar un nivell alt de risc, el que implicaria la necessitat de realitzar una AIPD; així com les metodologies

¹ Dictamen 1/2010 sobre els conceptes de "responsable del tractament" i "encarregat del tractament", del Grup de l'Article 29 sobre protecció de dades, adoptat el 16 de febrer de 2010, 00264/10/ES WP 169.

² Els criteris de risc tenen en compte principalment les previsions dels articles 32.1 i 2, 35.1, i 3, dels Considerants 71, 75, 83, 90 i 91 RGPD i de l'article 28 LOPDGDD.

³ Guia del Grup de treball de l'article 29 per a l'avaluació de l'impacte en la protecció de dades (DPIA) i per determinar si un tractament pot generar un alt risc als efectes del Reglament 2016/679, adoptat el 4 d'octubre de 2017, 17/EN WP248 rev.01.

i llistes de tractaments que requereixen la realització d'una AIPD, que s'han elaborat per part de les autoritats de protecció de dades⁴.

Així doncs, els criteris de risc per al tractament de dades personals que es tindran en compte al present MCPD són els següents:

- **Naturalesa de les dades (NAT):**

NAT.1. **Categories especials de dades:** S'inclouen en aquest criteri les categories especials de dades personals, que són aquelles que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical i el tractament de dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o les orientacions sexuals d'una persona física (art. 9.1 RGPD), les dades personals relatives a condemnes i infraccions penals (art. 10 RGPD), així com les dades relacionades amb la comissió d'infraccions administratives (art. 28.2.c LOPDGDD).

Adicionalment s'inclouran en aquest criteri altres categories de dades que augmentin el possible risc pels drets i llibertats de les persones, com les que permetin determinar la situació financera o de solvència patrimonial de les persones, o deduir informació sobre les persones relacionada amb categories especials de dades.

NAT.2. **Dades de col·lectius vulnerables:** Aquest criteri es basa en l'impacte que pot tenir l'activitat d'un determinat tractament sobre persones que estiguin en situació de desequilibri front el responsable del tractament o en persones que estiguin en una situació de risc d'exclusió social. Serien persones que no poden decidir sobre el tractament de dades o no poden exercir els seus drets degut a aquesta situació d'especial vulnerabilitat, com poden ser persones amb discapacitats, menors, pacients o presos (Article 28.2.e LOPDGDD, Considerant 75 RGPD).

- **Abast del tractament (ABT):**

ABT.1. **Tractament de dades a gran escala:** el RGPD no defineix el terme "a gran escala", encara que el Considerant 91 del citat reglament ofereix alguns factors que es poden tenir en compte a l'hora de determinar si el tractament es realitza a gran escala:

- a) el nombre d'interessats afectats, bé com a xifra concreta o com a proporció d'una determinada població;
- b) el volum de dades o la varietat de dades diferents que es processen;
- c) la durada, o permanència, de l'activitat de tractament de dades;
- d) l'abast geogràfic de l'activitat de tractament.

⁴ Llista de tipus de tractaments de dades que requereixen Avaluació d'Impacte relativa a la Protecció de Dades, publicada per l'Autoritat Catalana de Protecció de Dades (APDCAT) i per l'Agència Espanyola de Protecció de Dades (AEPD), d'acord amb el que estableix l'art. 35.4 RGPD, setembre de 2019.

- ABT.2. **Varietat de dades de l'activitat de tractament:** Els principis de la protecció de dades s'apliquen a tota la informació relativa a una persona física identificada o identificable (Considerant 26 RGPD). Per tant, si l'activitat executa tractaments de dades amb un ampli nombre de dades que pugui identificar (o potencialment identificar) l'interessat pot comportar un risc en la protecció de dades.
- ABT.3. **Accés a la informació:** En avaluar el risc en relació amb la seguretat de les dades personals, cal tenir en compte els riscos que es deriven del tractament, "especialment com a conseqüència de la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades" (art. 32.2 RGPD). Per tant quan en relació amb una activitat de tractament hi hagi un nombre elevat d'unitats que accedeixen a la informació de l'activitat en qüestió, s'haurà de considerar el risc esmentat.
- ABT.4. **Transferències fora de l'Espai Econòmic Europeu** (en endavant, EEE): Si les dades personals es transfereixen de la Unió a tercers països o a organitzacions internacionals fora l'EEE, això podria comportar un risc si no es garanteix una protecció equiparable a la que atorga el RGPD. En aquest sentit, s'ha de valorar especialment si s'ha considerat que els països o organitzacions internacionals, als quals es transfereixen dades amb caràcter habitual, garanteixen un nivell adequat de protecció, mitjançant una decisió d'adequació de la Comissió Europea (article 28.2.g LOPDGD).

- **Context del tractament (CXT):**

- CXT.1. **Utilització de noves tecnologies o ús innovador de tecnologies consolidades:** La utilització d'una nova tecnologia o un ús innovador de les tecnologies existents consolidades, com potser la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb unes altres (p.ex. una combinació d'empremta dactilar i reconeixement facial) poden comportar riscos pels drets i llibertats de les persones, ja que podrien implicar noves formes de recollida i utilització de les dades (art. 35.1 RGPD).
- CXT.2. **Associació o combinació de conjunts de dades:** En aquest criteri s'inclou el risc vinculat a aquells tractaments de dades que impliquin l'associació, combinació o enllaç de registres de bases de dades (p.ex. procedents de dos o més tractaments realitzats amb diferents finalitats o per responsables del tractament diferents d'una manera que excedeixi les expectatives raonables de l'interessat).
- CXT.3. **Període de conservació de dades:** El RGPD estableix el principi de limitació del termini de conservació de les dades, de manera que no podran conservar-se més temps del necessari per les finalitats perseguides amb el tractament (art. 5.1.e RGPD). Per avaluar el nivell de seguretat el RGPD indica que s'han de tenir en compte els riscos del tractament com conseqüència de la destrucció, pèrdua o alteració de dades transmeses, conservades o tractades d'altra forma (art. 32.2 RGPD). Per tant, s'ha de tenir en compte el termini de conservació per valorar el risc que comporta aquesta operació de tractament pels drets i llibertats de les persones.

CXT.4. **Existència d'encarregats de tractament:** L'existència d'una persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracti dades personals per compte del responsable del tractament (el que es coneix com a encarregat del tractament segons es defineix a l'art. 4.8 RGPD) pot implicar un risc, ja que comportaria una pèrdua de control per part del responsable sobre el tractament i un augment de la possibilitat de fuga d'informació i accés no autoritzat a les dades (art. 32.2 RGPD).

CXT.5. **Comunicacions de dades:** La comunicació de dades és una operació de tractament que comporta un risc ja que suposa la pèrdua de control per part del responsable sobre les dades. La transmissió de dades fora de l'organització del responsable implicarà un risc per la possibilitat d'accés no autoritzat a les dades (art. 32.2 RGPD).

- **Finalitats del tractament (FIN):**

FIN.1. **Avaluació o *scoring*:** L'elaboració de perfils es defineix com "qualsevol forma de tractament automatitzat de dades personals consistent a utilitzar aquestes dades per avaluar determinats aspectes personals d'una persona física; en especial, per analitzar o predir aspectes relatius al rendiment professional, la situació econòmica, la salut, les preferències personals, els interessos, la fiabilitat, el comportament, la ubicació o els moviments d'aquesta persona" (art. 4.4 RGPD). Aquest tractament es menciona a la normativa com un dels susceptibles de generar riscos pels drets i llibertats de les persones i que podrien generar perjudicis a les mateixes (art. 28.2.d LOPDGDD, Considerants 75, 91 RGPD).

FIN.2. **Tractament de dades que impedeix l'exercici de drets o utilitzar un servei o executar un contracte:** Quan el tractament impedeixi als interessats l'exercici dels seus drets, l'accés a serveis, o l'execució de contractes podrà comportar un risc pels drets i llibertats de les persones (art. 22 i Considerant 91 RGPD, art. 28.2.b LOPDGDD). Així mateix, es tindran en compte en aquest criteri aquells tractaments que puguin generar situacions d'especial impacte en els subjectes davant pèrdues de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altra perjudici significatiu en els afectats (art. 28.2.a LOPDGDD).

FIN.3. **Presa de decisions automatitzades:** Els tractaments de dades que impliquin la presa de decisions automatitzades o que contribueixin en gran mesura a la presa d'aquestes decisions i que produeixin efectes jurídics per a les persones físiques o que les afectin significativament de manera similar, pot comportar un risc pels drets i llibertats dels interessats (arts. 35.3.a RGPD), p. ex. quan el tractament pugui generar situacions de discriminació o d'exclusió contra les persones. Si el tractament té un impacte mínim o no té efectes en les persones no compliria amb aquest criteri.

FIN.4. **Observació sistemàtica:** Un tractament que persegueixi observar, monitorar, supervisar, geolocalitzar, avaluar o controlar als interessats, de forma sistemàtica i exhaustiva, es considera que comporta un risc pels drets i llibertats d'aquests (art.




35.3.c RGPD). El fet que la observació sigui sistemàtica s'interpreta com que es produeix d'acord amb un sistema predefinit, organitzat i metòdic- que té lloc com una part d'un pla general de recollida de dades i que es porta a terme com una part d'una estratègia⁵. Aquest tipus d'observació representa un risc perquè les dades personals poden ser recollides en circumstàncies en les quals els interessats poden no ser conscients de qui està recopilant les seves dades i com s'utilitzaran (com la recollida de dades i metadades a través de xarxes, aplicacions o el processament d'identificadors únics que permetin la identificació d'usuaris de serveis de la societat de la informació). A més, pot resultar impossible per a les persones evitar ser objecte d'aquest tipus de tractament, com en el cas en que es produeixi en espais d'accés públic.

⁵ Guia del Grup de Treball de l'Article 29 sobre el Delegat de Protecció de Dades, 16/EN WP 243 rev01, adoptada el 13 de desembre de 2016 i revisat el 5 d'abril de 2017.

04 ANÀLISI DE LES ACTIVITATS DE TRACTAMENT

La metodologia d'anàlisi de les activitats de tractament que es descriu en aquest apartat, permet analitzar l'afectació dels criteris de risc establerts a l'anterior apartat als diferents paràmetres o detalls de les activitats de tractament. Un cop considerats tots els elements de risc de cada tractament, facilita l'obtenció de la classificació global del nivell de risc per les activitats de tractament a analitzar.

Seguint els criteris del punt 3. *Criteris per la Classificació de Tractaments* i, per obtenir de forma agregada la classificació del nivell de risc per cada activitat de tractament, s'ha assignat una distribució de pesos a cadascun dels aspectes introduïts per la Fitxa de Tractament (que responen a les condicions del tractament de dades analitzat) i que comporten elements de risc en base als criteris definits, tal i com es mostra a la *Taula 1 – Nivell d'Impacte de les respostes a la Fitxa de Tractament*.

Valoració dels elements de risc	Representació de l'avaluació dels elements de risc	Descripció dels elements de risc
Nivell d'afectació BÀSIC		Són elements dels criteris de risc (punt 3 del present Marc) que no afecten significativament a la classificació del nivell de risc de l'activitat de tractament.
Nivell d'afectació MITJÀ		Són elements dels criteris de risc (punt 3 del present Marc) que afecten significativament, amb un nivell mitjà, a la classificació del nivell de risc de l'activitat de tractament.
Nivell d'afectació ALT		Són elements dels criteris de risc (punt 3 del present Marc) que afecten amb un nivell alt a la classificació del nivell de risc de l'activitat de tractament.

Taula 1 – Nivell d'Impacte de les respostes a la Fitxa de Tractament

A continuació es mostra l'assignació d'aquests pesos per cadascun dels blocs que conformen la Fitxa de Tractament i que, de forma agregada, classifiquen els tractaments amb un nivell de risc per cadascuna de les activitats analitzades.

No obstant, encara que l'exposició dels criteris es fa seguint l'estructura de la Fitxa de Tractament, aquests criteris es poden aplicar igualment encara que no s'utilitzi aquesta eina, sempre i quan s'analitzin els mateixos continguts relatius als tractaments. Així mateix, la proposta que es realitza de valoració dels diferents elements continguts a la Fitxa de Tractament poden ser adaptats a la situació concreta de l'activitat de tractament i a les necessitats de l'administració que realitzi la classificació. L'afectació que cada element té en el nivell de risc de l'activitat de tractament s'ha determinat en funció de l'impacte que aquest element pot tenir en els drets i llibertats dels titulars de les dades.








A la columna “Avaluació elements de risc” s’indiquen aquells punts de la Fitxa de Tractament que s’analitzen de forma conjunta pel càlcul agregat de la classificació del nivell de risc. D’aquesta manera, es facilita a l’analista la interpretació dels càlculs utilitzats. Malgrat aquestes indicacions, l’analista ha de verificar que es compleixi amb allò establert al RGPD i amb les pautes que puguin proporcionar les autoritats competents.

4.1 Informació General

El primer bloc proveeix la informació que contextualitza la informació bàsica de l’activitat de tractament. La informació recollida en aquest bloc no afecta de cap manera al nivell d’impacte o risc de l’activitat de tractament, ja que només proporciona dades informatives.

4.2 Activitat de Tractament

El segon bloc es centra bàsicament en identificar la varietat de les dades que tracta cada activitat de tractament. Com mostra la Taula 2 – Detall del bloc tipologia de les dades, la informació recollida afecta de manera directa al nivell d’impacte o risc de l’activitat de tractament.




Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
B.A	B.2.1	Varietat de Dades	 	ABT.2. Varietat de dades.	Quan la Varietat de Dades sigui igual o superior a 20, el nivell de risc serà mitjà . Si fos menor a 20, el nivell de risc serà bàsic .
B.B	B.2.2	Categories especials de dades o dades sensibles	  	NAT.1. Categories especials de dades.	Quan s’hagi marcat un nombre igual o major a 1 camp de les considerades categories especials de dades o dades sensibles i/o bé un nombre igual o major a 4 camps de les dades econòmiques, financeres i d’assegurances i/o s’hagin marcat dades relatives a l’“Historial financer” i/o la “Solvència patrimonial” s’eleva el risc a alt . En cas que, d’acord amb el previst a l’apartat anterior, s’hagi activat el risc alt, però s’hagi indicat que les dades són d’accés públic o bé que el tractament sigui merament incidental o accessori, el nivell de risc es reduirà a mitjà . Quan no es compleixi cap dels supòsits anteriors, el nivell de risc serà bàsic .
B.C	B.2.3	Dades biomètriques (identificació unívoca)	 	NAT.1. Categories especials de dades.	Quan s’hagi marcat dades biomètriques d’identificació unívoca s’activa el nivell alt . En cas contrari, el nivell de risc serà bàsic .

Grup Càlcul	ID Element de risc	Elements de risc	Avaluació o elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
B.D	B.2.4	Dades genètiques	 	NAT.1. Categories especials de dades.	Quan s'hagi marcat dades genètiques, s'activarà el nivell alt . En cas contrari, el nivell de risc serà bàsic .

Taula 2 – Detall del bloc tipologia de les dades

4.3 Característiques de l'activitat de tractament










El tercer bloc pretén identificar les característiques de l'activitat de tractament. Com mostra la *Taula 3 – Detall del bloc Característiques de l'activitat de tractament*, la informació recollida en aquest bloc afecta de forma directa al nivell de risc de l'activitat de tractament, ja que la implicació que l'activitat de tractament en qüestió processi dades a gran escala i la seva naturalesa sigui sensible, augmenta la probabilitat de materialització dels criteris del punt 3 del present Marc.

Grup Càlcul	ID Element de risc	Elements de risc	Avaluació o elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
C.A	C.1	Activitat de tractament a gran escala	  	ABT.1. Tractament de dades a gran escala.	<p>Quan s'hagi marcat l'opció "Més de 1.000.000"; o la combinació de les opcions "De 100.001 a 1.000.000 interessats" i "11-20 dades de cada interessat" o superior; o la combinació de les opcions "De 100.001 a 1.000.000 interessats" i "Entre 2 anys i 10 anys" o superior i "Àmbit mundial", el resultat serà alt.</p> <p>Quan s'hagi marcat l'opció "De 0 a 50.000 interessats" i alguna de les opcions "Entre 2 anys i 10 anys" o "Indefinit" i "Àmbit Europeu" o "Àmbit Mundial" i "més de 40 dades de cada interessat" o s'hagi marcat la combinació "De 50.001 a 100.000 interessats" i "21-40 dades de cada interessat" o superior o s'hagi marcat la combinació "De 50.001 a 100.000 interessats" i "11-20 dades de cada interessat" o superior i alguna de les dos opcions "Entre 2 anys i 10 anys" o "Indefinit", el resultat serà mitjà.</p> <p>Quan no es compleixi amb cap dels supòsits plantejats, el nivell de risc serà bàsic.</p>

Taula 3 – Detall del bloc Característiques de l'activitat de tractament

4.4 Descripció i finalitats de l'activitat de tractament




El quart bloc recull les finalitats de l'activitat de tractament. Com mostra la *Taula 4 – Detall del bloc Descripció i Finalitats*, la informació recollida en aquest bloc afecta de forma directa al nivell d'impacte o risc de l'activitat de tractament, concretament si s'executa qualsevol de les següents activitats: elaboració de perfils, presa de decisions automatitzades, impediment d'exercici de drets, accés a serveis o contractes o observació sistemàtica.

Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
D.A	D.2	Tipologia de finalitats i usos previstos de l'activitat de tractament	  	FIN.2. Tractament que impedeix drets.	Al respecte de la Fitxa de Tractament, les següents opcions de finalitats: "Toxicomanies", "Investigació epidemiològica", "Assistència sanitària", "Procediments judicials", "Inspecció i protecció social", "Prestació garantia salarial", "Prestacions assistència social", "Gestió de sancions", "Ajuts i subvencions", "Procediments i registres administratius", "Gestió i control sanitari", "Discapacitats/Dependències", "Recaptació tributària", "Altres serveis socials" o "Educació especial" elevaran el nivell de risc a mitjà .
	D.5	Tractament que impedeix drets			Quan a la pregunta D.5 s'hagi marcat la opció "Sí" el nivell serà alt . En cas que no s'activi ni el nivell mitjà ni l'alt, el nivell de risc serà bàsic .
D.B	D.3	Elaboració de perfils	 	FIN.1. Avaluació o scoring.	Quan la resposta d'aquesta pregunta sigui "Sí", el nivell de risc serà alt . En cas contrari, el nivell de risc serà bàsic .
D.C	D.4	Decisions automatitzades	 	FIN.3. Presa de decisions automatitzada.	Quan la resposta d'aquesta pregunta sigui "Sí", el nivell de risc serà alt . En cas contrari, el nivell de risc serà bàsic .
D.D	D.6	Observació sistemàtica	 	FIN.4. Observació sistemàtica.	Quan la resposta d'aquesta pregunta sigui "Sí", el nivell de risc serà alt . En cas contrari, el nivell de risc serà bàsic .

Taula 4 – Detall del bloc Descripció i Finalitats

4.5 Col·lectius d'interessats




El bloc E de la Fitxa de Tractament, com presenta la *Taula 5 – Detall del bloc col·lectius d'interessats*, proveeix informació sobre si el tractament inclou dades relatives a interessats vulnerables.





Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
E.A	E.1	Col·lectius d'interessats	  	NAT.2. Col·lectius vulnerables.	Quan la categoria d'interessats coincideixi amb les categories d'“Empleats”, “Demandants d'ocupació”, “Immigrants”, “Sol·licitants” o “Beneficiaris” es marcarà com a nivell de risc mitjà . Si hi ha un o més col·lectius vulnerables, el nivell de risc serà alt . En cas que no es compleixi cap dels supòsits anteriors, el nivell de risc serà bàsic .

Taula 5 – Detall del bloc col·lectius d'interessats

4.6 Context de tractament

El bloc F, en aquest cas, tal com mostra la *Taula 6 – Detall del bloc Context del tractament* proveeix informació sobre el context de l'activitat de tractament. Es defineix com a context aquells elements del tractament que condicionen com es duu a terme (com per exemple els sistemes de tractament utilitzats per processar les dades de l'activitat de tractament en qüestió). En relació a aquest aspecte, serà important saber si aquests sistemes formen part d'una solució tecnològica innovadora.









Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
F.A	F.2	Noves tecnologies o ús innovador	  	CXT.1. Noves tecnologies o ús innovador.	Si el tractament emprava tecnologia basada en “Dispositius mèdics connectats” o “Tècniques genètiques”, o bé dues o més solucions tecnològiques de les incloses en aquest apartat l'element de risc resultarà amb un nivell alt . Quan s'hagi marcat qualsevol de les altres opcions i només s'emprava una tecnologia la resposta serà de nivell mitjà . Si no es marca cap de les tecnologies, el nivell de risc serà bàsic .

Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
F.B	F.3	Combinació de conjunts de dades	 	CXT.2. Combinació de conjunts de dades.	Quan la resposta d'aquesta pregunta sigui "Sí", el nivell de risc serà alt . En cas contrari, el nivell de risc serà bàsic .
F.C	F.4	Període de conservació de dades	 	CXT.3. Període de conservació de dades.	Quan les opcions "10 o més anys" o "Permanent" s'hagin marcat, la resposta serà de nivell mitjà . En cas contrari, el nivell de risc serà bàsic .

Taula 6 – Detall del bloc Context del tractament

4.7 Model de Tractament

Finalment, pel que fa a l'últim bloc, tal i com es mostra a la *Taula 7 – Detall del bloc Model de Tractament*, es recull la informació necessària referent a l'accés a la informació per part d'altres unitats, la comunicació de dades, transferències internacionals de dades, així com l'existència d'encarregats del tractament.

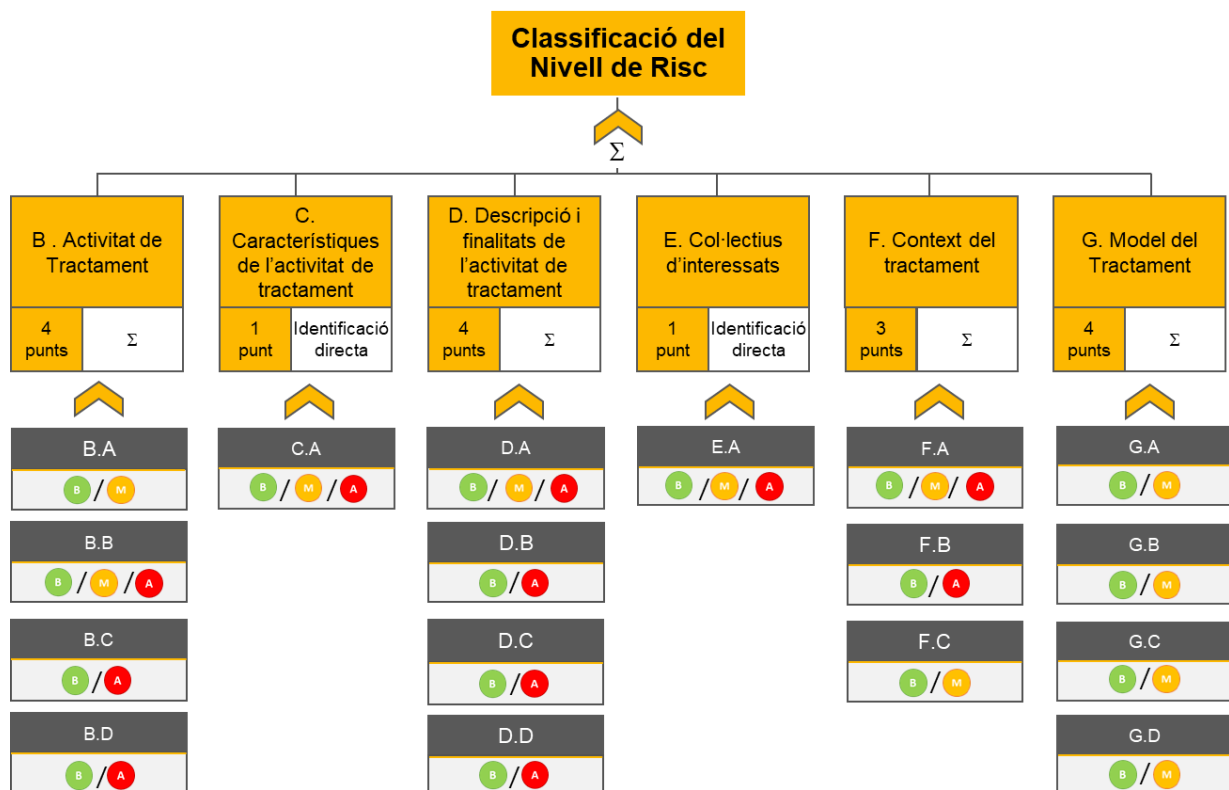
Grup Càlcul	ID Element de risc	Elements de risc	Avaluació elements de risc	Criteris per a la Classificació de Tractaments	Càlcul / Comentaris
G.A	G.1	Nombre d'unitats administratives que accedeixen	 	ABT.3. Accés a la Informació.	Quan el nombre d'unitats administratives que accedeixen a les dades sigui igual o superior a 50 unitats, el risc serà mitjà . Si és inferior, el nivell de risc serà bàsic .
G.B	G.2	Nombre de comunicacions de dades	 	CXT.5. Comunicacions de dades.	Quan el nombre de comunicacions de dades sigui igual o superior a 5 el risc serà mitjà . Si és inferior, el nivell de risc serà bàsic .
G.C	G.4	Nombre d'encarregats de tractament	 	CXT.4. Existència d'encarregats de tractament.	Quan el nombre d'encarregats sigui igual o superior a 5 encarregats identificats, el risc augmentarà a mitjà per aquesta agrupació. Si és inferior, el nivell de risc serà bàsic .
G.D	G.6	Transferències fora l'Espai Econòmic Europeu	 	ABT.4. Transferències fora l'Espai Econòmic Europeu.	Quan s'hagi marcat un país fora de l'EEE respecte del qual no s'hagi declarat una decisió d'adequació i es realitzin amb caràcter habitual, el nivell de risc serà mitjà . En cas que existeixi transferència i es realitzi en virtut d'una decisió d'adequació o que no existeixi transferència internacional de dades o que la transferència no sigui amb caràcter habitual, el nivell de risc serà bàsic .

Taula 7 – Detall del bloc Model de Tractament

05 DEFINICIÓ DE LA CLASSIFICACIÓ DEL NIVELL DE RISC

L'objectiu d'aquest punt és definir la classificació del nivell de risc associat a les activitats de tractament dels Departaments de la Generalitat de Catalunya i que marcarà l'aplicació de les mesures de ciberseguretat a implementar. Les mesures de ciberseguretat exigibles als tractaments de dades personals es determinen d'acord amb la classificació de risc elaborada per a cada tractament (segons les valoracions parcials esmentades a l'apartat anterior). La classificació es materialitza en tres nivells de risc globals: Bàsic, Mitjà i Alt.























Per a classificar el nivell global de risc d'un tractament s'analitzarà la informació recollida per cada tractament, identificant els nivells per cadascuna de les agregacions dels blocs anteriorment identificats amb color gris. Un cop calculats es sumaran per obtenir un únic nivell de risc per cada activitat de tractament. A la següent *Il·lustració 2 - Càlcul per a la definició de la classificació del nivell de risc* es mostra com s'haurà d'identificar directament o sumar.



Il·lustració 2 - Càlcul per a la definició de la classificació del nivell de risc

La classificació de cada tractament en un d'aquests nivells de risc permetrà a la Generalitat de Catalunya, tenint en compte l'estat de la tècnica i els costos d'aplicació, aplicar mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc (article 32.1 RGPD).

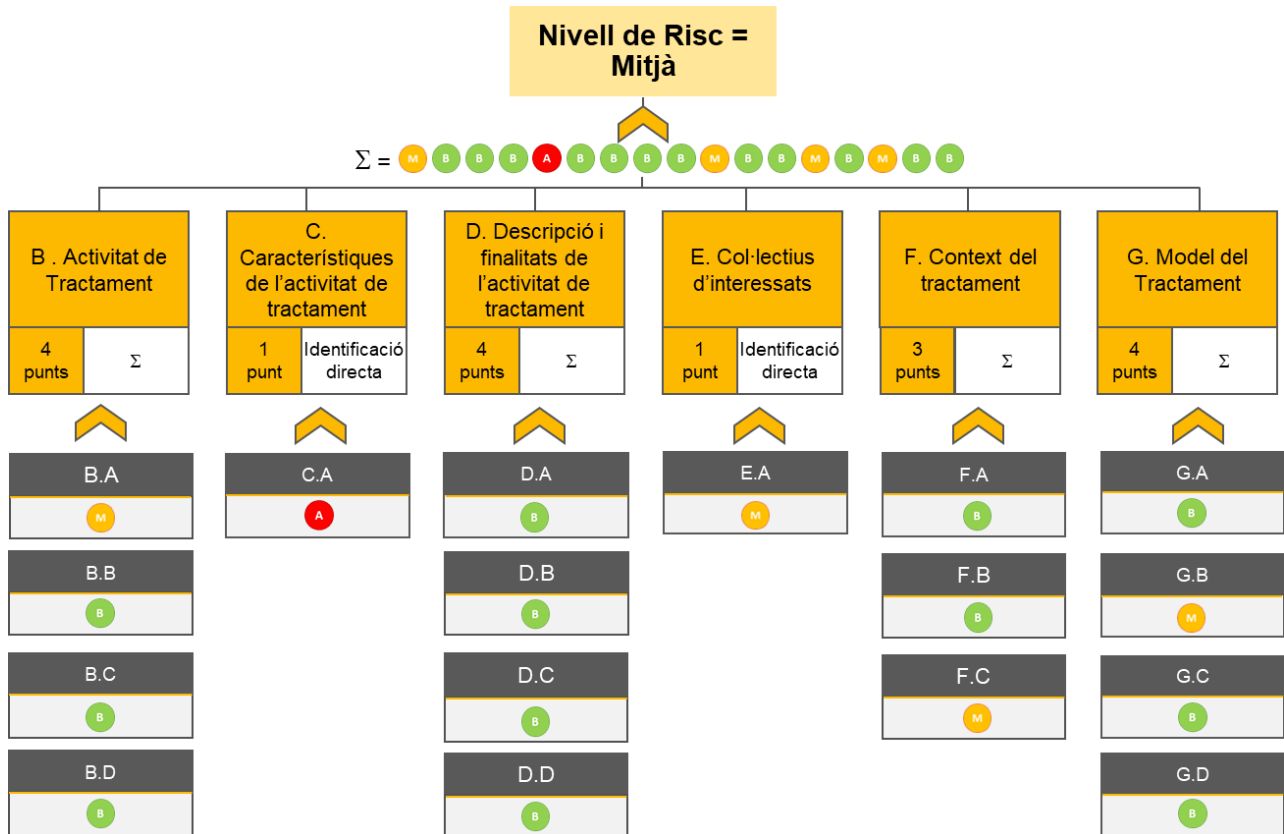
La *Taula 8 – Classificació del nivell de risc* mostra els tres nivells de risc i el seu càlcul, basat en el comptador de punts d'afectació per a cada activitat de tractament.

Nivell de risc	Càlcul del nivell de risc	Descripció dels nivells de risc
Alt	<p>El nivell de risc per cada activitat de tractament resultarà ser Alt quan es compleixi qualsevol de les següents casuístiques:</p> <p>(2)  +  o superior</p> <p>(1)  i (7)  +  +  +  +  +  +  o superior</p>	<p>Resultarà ser de nivell Alt quan resultin dos o més grups de càlcul de nivell alt o quan s'activi la combinació d'un grup de càlcul de nivell Alt i set o més grups de càlcul de nivell mitjà.</p>
Mitjà	<p>El nivell de risc per cada activitat de tractament resultarà ser Mitjà quan es compleixi qualsevol de les casuístiques que es trobin entre els següents llindars:</p> <p>(1)  i (6)  +  +  +  +  + </p> <p>(3)  +  +  o superior</p>	<p>Resultarà de nivell Mitjà quan es compleixi alguna de les casuístiques que es trobin entre els llindars indicats.</p>
Bàsic	<p>(2)  +  o inferior</p>	<p>Quan no s'activi cap dels escenaris anteriors i s'activin com a màxim dos grups de càlcul de nivell mitjà l'activitat de tractament resultarà ser de nivell bàsic.</p>

Taula 8 – Classificació del nivell de risc

5.1 Exemple per a la definició de la classificació del nivell de risc

Per tal de clarificar l'execució del càlcul i, per tant, l'obtenció del nivell de risc de cada una de les activitats de tractament analitzades, seguidament a la *II-lustració 3 - Exemple per a la classificació del nivell de risc* es mostra a través de la metodologia presentada anteriorment un possible conjunt de resultats que fan obtenir el nivell de risc per cada una de les agrupacions de càlcul.



II-lustració 3 - Exemple per a la classificació del nivell de risc

L'exemple mostra com aquesta activitat de tractament obté una agrupació de càlcul de nivell de risc alt i quatre de nivell mitjà. Per tant el nivell de l'activitat de tractament resulta ser **mitjà** segons el que s'especifica a la *Taula 8 – Classificació del nivell de risc*.



www.ciberseguretat.cat

