UNITAT 3

LES ADMINISTRACIONS PÚBLIQUES COM A RESPONSABLES EN L'RGPD. RELACIONS AMB ELS SEUS ENCARREGATS DE TRACTAMENTS

CONTINGUTS

1. **El principi de responsabilitat activa**
2. **Relacions responsable vs encarregat. Referència especial a les administracions públiques**
3. **Privacitat des del disseny i per defecte**
4. **Del registre de fitxers al registre d'activitats del tractament**
5. **La seguretat en l'RGPD**
6. **Enfocament i anàlisi del risc**
7. **Notificacions de violacions de seguretat**
8. **Avaluacions d'impacte de protecció de dades**

OBJECTIUS

1. **Enumerar les obligacions dels responsables del tractament per garantir el dret a la protecció de dades**
2. **Identificar els conceptes bàsics relacionats amb la seguretat de la informació de conformitat amb l'esquema nacional de seguretat**

3.1. El principi de responsabilitat activa

El CONCEPTE DE RESPONSABILITAT PROACTIVA s'estableix en l'article 5 de l'RGPD, en què es defineixen el conjunt de principis que s'han d'aplicar per protegir de manera efectiva les dades personals. En concret en l'apartat 2 s'estableix que la responsabilitat proactiva és una de les obligacions del responsable del tractament amb relació als principis que s'estableixen en l'apartat 1 del mateix article. Per tant, és una de les noves obligacions que s'estableixen en l'RGPD per assegurar que es compleixen aquests principis, i que consisteix en la capacitat del responsable, és a dir, de l'organització, de demostrar i proporcionar evidències d'aquest compliment.

El concepte de responsabilitat proactiva es perd en la traducció de l'RGPD, des de la redacció original en anglès fins a la traducció a l'espanyol. EN LA VERSIÓ EN ANGLÈS S'USA EL TERME *ACCOUNTABILITY*. Si ens remetem a la definició que trobam en el diccionari Oxford, *accountability* és la situació o l'estat pel qual està clarament identificat el responsable de les accions que es prenen en l'organització. I afegeix que, amb relació a aquestes accions, aquest responsable pot proporcionar una explicació, satisfactòria i demostrable, del perquè, i amb quina base legal o sobre quins principis, es van prendre aquestes accions.

L'RGPD introdueix un canvi important en la manera en què un responsable del tractament ha d'enfrontar-se a les seves obligacions amb relació a la protecció de dades de caràcter personal. ES BASA EN UN PRINCIPI D'AUTOANÀLISI, CRÍTIC, CONTINU, «TRAÇABLE» I BASAT EN LA RESPONSABILITAT, QUE PERMETI IMPLEMENTAR UNA VERITABLE GOVERNANÇA DE DADES PERSONALS AL SI DE LES EMPRESES. «Traçable» suposa que existeix un registre de les diferents decisions en el temps, fins i tot quan aquestes decisions han resultat contradictòries. Amb responsabilitat implica que en aquest registre s'identifica la persona que va prendre les decisions, o les que no va prendre quan ho hauria d'haver fet, per què va prendre aquestes decisions, quina justificació hi havia per prendre-les i quan les va prendre. A més, depenent del tipus d'activitat o decisió, es poden recollir dades addicionals que poden resultar rellevants per al procés de negoci, o per al servei proporcionat als subjectes de les dades, com on va prendre aquesta decisió, o des de quin dispositiu es va prendre aquesta decisió.

Un altre aspecte rellevant és que el principi de responsabilitat proactiva implica tot el personal de l'organització en el dia a dia del tractament de dades de caràcter personal. EL PERSONAL DE L'ORGANITZACIÓ HA D'ADOPTAR UNA ACTITUD PROACTIVA, COMPROMESA I RESPONSABLE, CONSCIENT DE LA NECESSITAT DE PRESERVAR UN DRET FONAMENTAL. En definitiva, una nova actitud activa en l'execució de les obligacions.

El conjunt de tasques que s'han d'implementar per fer efectiu el principi de responsabilitat proactiva amb relació a la protecció de dades de caràcter personal s'estén al llarg tot l'RGPD. Sense pretendre ser exhaustius, inclou les

mesures següents:

- La implementació del PRINCIPI DE TRANSPARÈNCIA.
- L'EXERCICI DELS DRETS reconeguts als interessats.
- L'obligació de disposar d'un DELEGAT DE PROTECCIÓ DE DADES.
- L'obligació de mantenir una LLISTA DE TRACTAMENTS, que substitueix la de la notificació de fitxers a l'Autoritat de Control.
- L'ANÀLISI DE RISCS DE SEGURETAT I LA DEFINICIÓ DELS REQUISITS DE PRIVACITAT DES DEL DISSENY I ELS DE PRIVACITAT PER DEFECTE.
- La IMPLEMENTACIÓ DE LES MESURES DE SEGURETAT IDENTIFICADES com a resultat de l'anàlisi de risc i la NOTIFICACIÓ DE LES VIOLACIONS DE SEGURETAT.
- L'obligació de fer quan correspongui una ANÀLISI D'IMPACTE A LA PRIVACITAT.
- La possible obtenció voluntària DE CERTIFICATS I DE SEGELLS DE PRIVACITAT, o l'ADHESIÓ A CODIS DE CONDUCTA.

La responsabilitat proactiva implica la configuració de l'organització des de la perspectiva de protecció de dades. És a dir, suposa introduir una cultura de protecció de dades en l'organització.

3.2. Relacions responsable vs encarregat. Especial referència a les administracions públiques

Per determinar les relacions entre el responsable del tractament i l'encarregat de tractament en l'àmbit de les administracions públiques, hem de partir, en primer lloc, de les definicions que estableix l'RGPD.

L'RGPD defineix, en l'article 4.7, com a «RESPONSABLE DEL TRACTAMENT» O «RESPONSABLE»:

> «La persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determina els fins i els mitjans del tractament; si el dret de la Unió o dels estats membres determina els fins i els mitjans del tractament, el responsable del tractament o els criteris específics per nomenar-lo podrà establir-los el dret de la Unió o dels estats membres.»

Respecte a la definició d'«ENCARREGAT DEL TRACTAMENT» o «ENCARREGAT», segons l'RGPD:

> «la persona física o jurídica, autoritat pública, servei o un altre organisme que tracta dades personals a compte del responsable del tractament».

En l'Administració, trobam els supòsits típics d'encarregats de tractament, com poden ser la contractació d'una empresa perquè destrueixi documents, o d'un servei de computació en el núvol, així com qualsevol altre que hagi estat contractat per l'Administració corresponent per prestar un servei que comporta un tractament de dades de caràcter personal.

Les obligacions generals que han de tenir-se en compte a l'hora de formalitzar

una relació entre el responsable del tractament i un prestador de serveis que sigui encarregat del tractament les defineix l'article 28 de l'RGPD. En particular, el contracte o acte d'encàrrec de tractament ha de contenir:

- Les instruccions del responsable del tractament.
- El deure de confidencialitat.
- Les mesures de seguretat.
- El règim de la subcontractació.
- La manera com l'encarregat assistirà el responsable en el compliment de l'obligació de respondre l'exercici dels drets dels interessats.
- La col·laboració en el compliment de les obligacions del responsable.
- El destí de les dades en finalitzar la prestació.

Per facilitar la formalització d'aquest tipus de contractes una vegada que és aplicable l'RGPD, l'AEPD en col·laboració amb l'Agència Basca de Protecció de Dades i l'Autoritat Catalana de Protecció de Dades, ha publicat el document «Directrius per a l'elaboració de contractes entre responsables i encarregats del tractament», que conté un annex amb un exemple de clàusules contractuals per als supòsits en què l'encarregat del tractament tracta les dades en els locals del responsable.

La Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals ha regulat de manera específica aquesta figura en l'article 33 i completa la regulació de l'RGPD:

> Article 33. Encarregat del tractament
> 1. L'accés per part d'un encarregat de tractament a les dades personals que resulten necessàries per prestar un servei al responsable no es considera comunicació de dades sempre que es compleixi el que estableix el Reglament (UE) 2016/679, en aquesta Llei orgànica i en les seves normes de desenvolupament.
> 2. Té la consideració de responsable del tractament i no la d'encarregat qui, en el seu propi nom i sense que consti que actua a compte d'un altre, estableixi relacions amb els afectats encara que existeixi un contracte o acte jurídic amb el contingut fixat en l'article 28.3 del Reglament (UE) 2016/679. Aquesta previsió no és aplicable als encàrrecs de tractament efectuats en el marc de la legislació de contractació del sector públic.
> Té també la consideració de responsable del tractament qui figuri com a encarregat i utilitzi les dades per a les seves pròpies finalitats.
> 3. El responsable del tractament ha de determinar si, quan finalitzi la prestació dels serveis de l'encarregat, les dades personals han de ser destruïdes, tornades al responsable o lliurades, si escau, a un nou encarregat.
> No és procedent destruir les dades quan existeixi una previsió legal que obligui a conservar-les, cas en el qual han de ser tornades al responsable, que n'ha de garantir la conservació mentre persisteixi aquesta obligació.
> 4. L'encarregat del tractament pot conservar, degudament bloquejades, les dades, sempre que es puguin derivar responsabilitats de la seva relació amb el responsable del tractament.
> 5. En l'àmbit del sector públic podran atribuir-se les competències pròpies d'un encarregat del tractament a un determinat òrgan de l'Administració General de l'Estat, l'Administració de les comunitats autònomes, les entitats que integren l'Administració local o els organismes que hi estan vinculats o que en depenen, adoptant una norma reguladora d'aquestes competències, que ha d'incorporar el contingut exigit per l'article 28.3 del Reglament (UE) 2016/679.

La regulació de la contractació de tercers prestadors de serveis en qualitat d'encarregat del tractament ha estat recentment actualitzada amb la reforma mitjançant Reial Decret llei 14/2019, de 31 d'octubre, de la Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014. Aquesta reforma excedeix els objectius d'aquest curs per la seva complexitat, però determina:

- L'obligació d'incloure una referència a la legislació aplicable al contracte, amb expressa menció a la submissió a la normativa nacional i de la Unió Europea en matèria de protecció de dades.

- La inclusió obligatòria en els plecs de clàusules administratives particulars dels elements següents:

  a) La finalitat per a la qual se cedeixen aquestes dades.[1]

  b) L'obligació del futur contractista de sotmetre's en qualsevol cas a la normativa nacional i de la Unió Europea en matèria de protecció de dades, sens perjudici del que estableix el darrer paràgraf de l'apartat 1 de l'article 202.

  c) L'obligació de l'empresa adjudicatària de presentar, abans de formalitzar el contracte, una declaració en què posa de manifest on estaran ubicats els servidors i des d'on es prestaran els serveis que hi estan associats.

  d) L'obligació de comunicar qualsevol canvi que es produeixi, durant la vigència del contracte, de la informació facilitada en la declaració a què es refereix la lletra *c)* anterior.

  e) L'obligació dels licitadors d'indicar en l'oferta, si tenen previst subcontractar els servidors o els serveis que hi estan associats, el nom o el perfil empresarial, definit amb referència a les condicions de solvència professional o tècnica, dels subcontractistes als quals s'encomani que ho facin.

- La consideració de les clàusules anteriors –*(a)-(e)*– com a essencials i causa de resolució del contracte.

- És possible no només la resolució per incomplir aquestes clàusules essencials. Existeix la prohibició de contractar les empreses el contracte de les quals hagi quedat resolt per incompliment culpable del contractista de les obligacions que els plecs han qualificat d'essencials.

1 Observau la incorrecció tècnica del legislador, ja que l'article 33 de la LOPDGDD exclou aquesta cessió.

En l'àmbit del sector públic definit per la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, és possible una relació entre responsable i encarregat a través d'una comanda de gestió, d'un conveni o contracte administratiu. En aquest darrer cas, la disposició addicional 25a de la Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014, determina que

> «En el cas que la contractació impliqui l'accés del contractista a dades de caràcter personal del tractament de les quals sigui responsable l'entitat contractant, aquell té la consideració d'encarregat del tractament», amb les especificitats establertes en tal disposició addicional. »

Tanmateix, el que entre entitats particulars quedava clar amb la signatura d'un contracte ha suscitat dubtes moltes vegades al si de les administracions públiques, en què sovint les estructures orgàniques assignen una/unes unitat/unitats, subdireccions generals/serveis/negociats, funcions de gestió, etc. a una altra unitat, subdirecció general d'informàtica, agència, etc. Entre aquestes funcions hi ha:

- El desenvolupament dels sistemes d'informació necessaris per al funcionament dels serveis, el portal web, la seu electrònica, la intranet, les eines col·laboratives i els dominis d'Internet del/de la [Ministeri/CA/Ajuntament].

- L'impuls de l'administració digital del/de la [Ministeri/CA/Ajuntament] i els seus organismes d'acord amb el pla d'acció departamental per a la transformació digital i l'Estratègia TIC de l'Administració, així com la provisió de serveis en matèria de tecnologies de la informació i comunicacions que li correspon prestar com a unitat TIC del/de la [Ministeri/CA/Ajuntament].

- L'impuls i la coordinació en l'àmbit del/de la [Ministeri/CA/Ajuntament] dels Esquemes Nacionals d'Interoperabilitat i Seguretat, i de les mesures per garantir l'accessibilitat dels serveis electrònics i el compliment de les seves obligacions, en matèria de reutilització de la informació del sector públic.

AIXÍ DONCS, MOLTES VEGADES APAREIXEN UNITATS TRANSVERSALS, AMB CONDICIÓ D'ENCARREGAT DE TRACTAMENT EN VIRTUT D'ATRIBUCIÓ DE COMPETÈNCIES[2] que apareixen reflectides en una norma de caràcter reglamentari organitzatiu, com un reial decret (Administració General de l'Estat) o decret (comunitat autònoma) d'estructura, o fins i tot en una llei quan s'ha creat un organisme específic per a això.

És a dir, ens trobam amb un organisme o entitat que actua com a encarregat de

2 Aquest supòsit específic ha estat analitzat per l'informe jurídic de l'AEPD següent: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2012-0333_Encargado-del-tratamiento-en-virtud-de-atribuci-oo-n-de-competencias..pdf

tractament en l'àmbit de la seva respectiva Administració pública, atès que se li atribueixen funcions i competències que no incideixen en el poder decisori sobre la finalitat, el contingut i l'ús de les dades, sinó que fonamentalment versen sobre la implantació i la utilització dels sistemes d'informació perquè siguin utilitzats pels òrgans i organismes corresponents.

Aquest supòsit específic, quan l'encarregat de tractament està configurat en funció d'aquestes normes de caràcter reglamentari organitzatiu, o fins i tot legals, que en fixen les competències, suposa ja l'existència d'un CONTRACTE d'encàrrec de tractament, sense que per tant sigui necessari formalitzar contractes específics per a cada òrgan o organisme en els termes de l'art. 12.2 de la LOPD. En aquest sentit, la reforma de la LOPD avui en tramitació, si s'aprova, en l'apartat 5 de l'article 33 té en compte aquesta situació així:

> «En l'àmbit del sector públic podran atribuir-se les competències pròpies d'un encarregat del tractament a un determinat òrgan de l'Administració General de l'Estat, l'Administració de les comunitats autònomes, les entitats que integren l'Administració local o els organismes que hi estan vinculats o que en depenen, adoptant una norma reguladora d'aquestes competències, que ha d'incorporar el contingut exigit per l'article 28.3 del Reglament (UE) 2016/679.»

D'altra banda, l'aplicació de l'RGPD no modifica les relacions entre responsable i encarregat o les qüestions que cal tenir en compte. El contingut mínim del contracte ha de contenir l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i categories d'interessats, i les obligacions i drets del responsable.

3.3. Privacitat des del disseny i per defecte

3.3.1. Introducció

En el text de l'RGPD es fa referència a dos principis per implementar de manera efectiva de la responsabilitat proactiva: la protecció de dades des del disseny i la protecció de dades per defecte. Aquestes referències se centren en els considerants 78 i 108 i en l'article 25, titulat «PROTECCIÓ DE DADES DES DEL DISSENY I PER DEFECTE», en què es configuren i desenvolupen aquests principis.

3.3.2. Protecció de dades des del disseny

De conformitat amb l'apartat 1 de l'article 25, es pot establir que el principi de PROTECCIÓ DE DADES DES DEL DISSENY té com a objectiu complir els requisits definits en l'RGPD i, per tant, els drets dels interessats. La protecció de dades ha d'estar present en les primeres fases de concepció d'un projecte i formar part de la llista d'elements que cal considerar abans d'iniciar etapes de desenvolupament successives.

Les mesures que permeten garantir la protecció de dades no són una capa afegida al tractament, un embolcall o una funcionalitat posterior, sinó que hi

estan íntimament incloses i en formen part integral de l'esperit del disseny, de manera que no són un element identificable que es pot llevar o posar, sinó que n'impregnen tota l'estructura. Per descomptat, aquests requisits es tradueixen en mesures tècniques i organitzatives amb l'objectiu d'aplicar de manera efectiva els principis de protecció de dades i integrar les garanties necessàries en el tractament. És important recalcar que la implementació d'un tractament no es basa únicament en un conjunt de productes de maquinari o programa, sinó que un tractament és un sistema format per màquines, persones, la interacció entre ambdues i els modes d'utilització i d'ús. Aquests darrers tres elements es defineixen en les mesures organitzatives.

> Un exemple d'aquestes mesures, que s'estableix de manera expressa en l'RGPD, és que el mateix tractament incorpori mesures per a la pseudoanonimització primerenca de les dades personals o la minimització de dades. La pseudoanonimització es defineix en l'apartat 5 de l'article 4 com el tractament de dades personals de tal manera que ja no puguin atribuir-se a un interessat sense utilitzar informació addicional, sempre que aquesta informació addicional figuri per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixin a una persona física identificada o identificable.

La minimització de dades no es troba explícitament definida en l'RGPD, però s'interpreta en el sentit que les dades personals objecte de tractament han de ser adequades, rellevants i limitades a les que siguin necessàries en relació amb la finalitat del tractament.

> Recordem que molts tractaments se segueixen fent en paper, una part fent còpies o utilitzant el suport d'impressió com còpies temporals de treball, i que aquesta forma de treball s'ha de tenir en compte a l'hora de dissenyar el procés global.

L'OBLIGACIÓ QUE S'ADOPTIN ELS PRINCIPIS DE PRIVACITAT DES DEL DISSENY RECAU EN EL RESPONSABLE DEL TRACTAMENT. El responsable del tractament pot subcontractar tant el desenvolupament com la implementació d'una part o de la totalitat del tractament. En aquest cas, complint les seves obligacions, ha de reflectir contractualment els requisits que garanteixen la protecció dels drets dels subjectes de les dades i fer el seguiment que aquests requisits han estat efectivament traduïts a decisions de disseny i que són funcionals. En el cas d'adquisició de productes o contractació de serveis que siguin utilitzats per implementar un tractament, entre els elements que s'utilitzen per determinar quin es tria entre els disponibles en el mercat ha de figurar, amb un pes significatiu, si no crític, el fet que es pugui demostrar que a l'hora de desenvolupar-lo s'han implementat els principis de privacitat des del disseny.

Sigui quina sigui la forma de subcontractació o adquisició, el responsable mai no pot delegar completament l'obligació d'aplicar aquest principi, ja que sempre quedaran sota el seu poder de decisió almenys les mesures organitzatives que li competeix prendre per interaccionar amb el servei subcontractat.

La selecció de les mesures és el resultat d'una anàlisi de riscs amb relació a la

probabilitat i la gravetat que afectin els drets i les llibertats de les persones físiques i s'apliquen tenint en compte l'estat de la tècnica, el cost d'aplicació i la naturalesa, l'àmbit, el context i els fins del tractament.

3.3.3. Privacitat per defecte

El CONCEPTE DE PRIVACITAT PER DEFECTE ES DESENVOLUPA en l'apartat 2 del mateix article 25. La idea principal és que només han de ser objecte de tractament les dades personals que siguin estrictament necessàries per a cadascun dels fins de tractament. Si és possible per la naturalesa del procés, cal arribar fins i tot a no tractar dades de caràcter personal.

En particular, es destaca com un dels principis dins la privacitat per defecte el fet que les dades personals no siguin accessibles a un nombre indeterminat de persones físiques, sense la intervenció del subjecte de les dades. Cal tenir en compte que el Reglament assenyala «persones físiques», no entitats, ja que es refereix a l'aplicació del principi de seguretat denominat «necessitat de conèixer» (*need-to-know*), com una nova extensió d'aquest principi que podríem denominar «necessitat de revelar» (*need-to-disclosure*).

> El principi de necessitat de conèixer estableix que en una organització les persones han de tenir accés només a la informació necessària per executar les seves tasques. El principi s'aplica a la protecció de dades de caràcter personal en la mesura que els empleats de l'empresa només han de tenir accés a les dades de caràcter personal que són estrictament necessàries per fer el seu treball o proporcionar un servei. El principi de necessitat de revelar té el mateix fonament, però estès a tercers que d'alguna manera estan relacionats amb el producte o servei sol·licitat, com podria ser el cas d'usuaris que han utilitzat el mateix servei, han estat en el mateix lloc o es troben en una mateixa situació.

Quatre estratègies bàsiques permeten implementar la privacitat per defecte:

- Recollida de dades: analitzar els tipus de dades que es recullen amb un criteri de minimització en funció dels productes i els serveis seleccionats per l'usuari;

- Tractament de les dades: analitzar els processos associats a aquests tractaments perquè s'accedeixi a les mínimes dades personals necessàries per executar-los;

- Conservació: implementar una política de conservació de dades que permeti, amb un criteri restrictiu, eliminar les dades que no siguin estrictament necessàries;

- Accessibilitat: limitar l'accés per part de tercers a aquestes dades personals.

Com en el cas de la privacitat des del disseny, aquests requisits es tradueixen en mesures tant tècniques com organitzatives i, en el cas de la privacitat per

defecte, és necessari posar fins i tot més atenció a aquestes darreres. Fins i tot, s'assenyala l'oportunitat de donar transparència a la implementació d'aquests tractaments i així permetre als interessats supervisar el procés de les seves dades i al responsable del tractament crear i millorar elements de seguretat.

3.4. Del registre de fitxers al registre d'activitats del tractament

A partir del 25 de maig de 2018, ha desaparegut la notificació de fitxers davant el Registre general de protecció de dades. Per bé que aquesta inscripció de fitxers desapareix, l'RGPD regula en l'article 30 el denominat «REGISTRE D'ACTIVITATS DE TRACTAMENT» així:

> 1. Cada responsable i, si escau, el seu representant han de mantenir un registre de les activitats de tractament que es duen a terme sota la seva responsabilitat. Aquest registre ha de contenir tota la informació que s'indica a continuació:
> *a)* el nom i les dades de contacte del responsable i, si escau, del corresponsable, del representant del responsable, i del delegat de protecció de dades;
> *b)* els fins del tractament;
> *c)* una descripció de les categories d'interessats i de les categories de dades personals;
> *d)* les categories de destinataris a què es van comunicar o es comunicaran les dades personals, incloent-hi els destinataris en tercers països o organitzacions internacionals;
> *e)* si escau, les transferències de dades personals a un tercer país o una organització internacional, incloent-hi la identificació d'aquest tercer país o organització internacional i, en el cas de les transferències indicades en l'article 49, apartat 1, paràgraf segon, la documentació de garanties adequades;
> *f)* quan sigui possible, els terminis prevists per a la supressió de les diferents categories de dades;
> *g)* quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat a què es refereix l'article 32, apartat 1.[3]
> 2. Cada encarregat i, si escau, el representant de l'encarregat han de mantenir un registre de totes les categories d'activitats de tractament que s'han duit a terme a compte d'un responsable que contengui:
> *a)* el nom i les dades de contacte de l'encarregat o encarregats i de cada responsable a compte del qual actuï l'encarregat i, si escau, del representant del responsable o de l'encarregat, i del delegat de protecció de dades;
> *b)* les categories de tractaments duits a terme a compte de cada responsable;
> *c)* si escau, les transferències de dades personals a un tercer país o una organització internacional, incloent-hi la identificació d'aquest tercer país o organització internacional i, en el cas de les transferències indicades en l'article 49, apartat 1, paràgraf segon, la documentació de garanties adequades;
> *d)* quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat a què es refereix l'article 30, apartat 1.
> 3. Els registres a què es refereixen els apartats 1 i 2 han de constar per escrit, incloent-hi en format electrònic.
> 4. El responsable o l'encarregat del tractament i, si escau, el representant del responsable o de l'encarregat han de posar el registre a disposició de l'autoritat de control que li ho sol·liciti.
> 5. Les obligacions indicades en els apartats 1 i 2 no s'apliquen a cap empresa ni organització que ocupi menys de 250 persones, llevat que el tractament pugui comportar un risc per als drets i les llibertats dels interessats, no sigui ocasional, o

3 En el cas d'Espanya, les mesures de seguretat que han d'adoptar els responsables i/o els encarregats de tractament del sector públic [l'article 2 de la Llei 40/2015] s'han d'entendre dins l'Esquema Nacional de Seguretat com especifica la disposició addicional primera del Projecte de Llei orgànica de protecció de dades.

> inclogui categories especials de dades personals indicades en l'article 9, apartat 1, o dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10.

És en aquest punt on l'existència del Registre de fitxers pot convertir-se en una eina d'ajuda i un punt de partida per a la tasca que ara ha d'emprendre.

Aquesta matèria ha estat complementada per l'article 31 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. Aquest precepte disposa en l'incís segon del paràgraf primer que:

> El registre, que pot organitzar-se al voltant de conjunts estructurats de dades, ha d'especificar, segons les seves finalitats, les activitats de tractament duites a terme i les altres circumstàncies establertes en el Reglament.

En la pràctica, això permet mantenir l'estructura tradicional en fitxers sota un nou criteri d'agregació. D'altra banda, el paràgraf segon assenyala:

> 2. Els subjectes enumerats en l'article 77.1 d'aquesta Llei orgànica han de fer públic un inventari de les seves activitats de tractament accessible per mitjans electrònics en què ha de constar la informació establerta en l'article 30 del Reglament (UE) 2016/679 i la seva base legal.

Aquesta previsió s'ha articulat mitjançant una reforma de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern, en la disposició addicional final onzena de la LOPDGDD:

> Disposició final onzena. Modificació de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
> Es modifica la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern, en els termes següents:
> U. S'hi afegeix un nou article 6 bis, amb la redacció següent:
> «Article 6 bis. Registre d'activitats de tractament.
> Els subjectes enumerats en l'article 77.1 de la Llei orgànica de protecció de dades personals i garantia dels drets digitals han de publicar el seu inventari d'activitats de tractament en aplicació de l'article 31 de la Llei orgànica esmentada.»

3.5. La seguretat en l'RGPD

3.5.1. Introducció

Les mesures de seguretat són eines que permeten assolir l'objectiu de protegir la informació. La seguretat de les dades personals té, almenys, dos enfocaments: un és el que correspon als responsables dels tractaments i l'altre és el que correspon als propis mateixos i interessats. .

3.5.2. Principis bàsics de la seguretat

Les mesures de seguretat són clau a l'hora de garantir el dret fonamental a la protecció de dades. No és possible garantir aquest dret fonamental sense garantir la confidencialitat, la integritat i la disponibilitat de les nostres dades. Per garantir aquests tres factors de la seguretat són necessàries mesures d'índole tant tècnica com organitzativa. A més, a vegades serà també necessari tenir en compte mesures de seguretat física com la presència d'un servei de seguretat o un sistema de control d'accessos que ens asseguri qui són les persones o processos que accedeixen a la informació en un moment determinat.

Quan ens referim a CONFIDENCIALITAT ens referim a qualsevol mesura que impedeixi l'accés no autoritzat a les dades personals, mecanismes per evitar la vulneració del deure de secret o mesures encaminades a garantir els privilegis d'accés a la informació o les dades personals.

> Per exemple, parlam de mesures per les quals es concedeixen o deneguen els permisos per accedir a un sistema d'informació o la gestió de les altes i baixes del personal d'una organització. En l'àmbit de la seguretat es vincula la confidencialitat amb el principi de la necessitat de saber, mitjançant el qual únicament han d'accedir a la informació les persones que ho necessiten en virtut de les funcions que han de desenvolupar en la seva feina o el seu càrrec.

La INTEGRITAT de les dades personals o de la informació es relaciona amb el principi d'exactitud o de qualitat de les dades. D'acord amb aquest principi, el responsable del tractament de les dades ha de garantir que les dades que es tracten concorden amb la realitat o són veraces i adequades a la finalitat per a la qual van ser obtingudes i, a més, se'n garanteix la inalterabilitat.

La DISPONIBILITAT és la característica de la seguretat per la qual s'intenta mantenir les dades accessibles per consultar-les, localitzar-les i rectificar-les quan sigui necessari. En altres paraules, aquesta característica garanteix els drets d'accés, rectificació i supressió, el dret de limitació del tractament i el dret a la portabilitat de les dades. En definitiva es tracta d'una característica de la seguretat estretament vinculada als drets dels interessats.

A les característiques generals de la seguretat esmentades anteriorment (confidencialitat, integritat i disponibilitat), l'RGPD hi afegeix la RESILIÈNCIA dels sistemes i serveis de tractament. L'RGPD defineix la resiliència com la

característica de la seguretat que permet garantir la confidencialitat, la integritat i la disponibilitat dels tractaments de dades personals, és a dir, la característica de la seguretat per la qual podem garantir la continuïtat d'un sistema d'informació o servei d'un tractament de dades personals en condicions adverses.

> Quan el sistema d'informació o servei del tractament de dades personals no és capaç de garantir el seu funcionament es produeix una pèrdua de servei, com en cas d'un ciberatac. Un altre dels paràmetres o característiques de la seguretat en l'RGPD és la capacitat de restaurar la tornada a la normalitat del sistema d'informació o servei de tractament, o la capacitat de recuperar el funcionament normal del sistema d'informació o servei de tractament.

3.5.3. RGPD i seguretat

L'article 32 de l'RGPD estableix que les mesures tècniques i organitzatives apropiades per garantir el nivell de seguretat adequat al risc es defineixen en funció de l'estat de la tècnica, els costos d'aplicació, i la naturalesa, l'abast, el context i els fins del tractament així com els riscs de probabilitat i gravetat variables per als drets i les llibertats de les persones. No s'estableixen mesures de seguretat estàtiques. Correspon al responsable determinar les mesures de seguretat que són necessàries per garantir la confidencialitat, la integritat i la disponibilitat de les dades personals. Per tant, un mateix tractament de dades pot implicar mesures de seguretat diferents en funció de les especificitats concretes d'aquest tractament de dades.

En definitiva, el primer pas per determinar les mesures de seguretat és l'AVALUACIÓ DEL RISC. Una vegada avaluat el risc és necessari determinar les mesures de seguretat encaminades a reduir o eliminar els riscs per al tractament de les dades.

Per acreditar el compliment dels requisits de seguretat que estableix l'RGPD, l'article 32.3 permet als responsables dels tractaments la possibilitat d'utilitzar MECANISMES DE CERTIFICACIÓ per garantir i demostrar el compliment dels requisits de seguretat, o l'adopció d'un CODI DE CONDUCTA. La certificació i els codis de conducta poden ser eines útils per complir el que preveu l'RGPD pel que fa a mesures de seguretat, però no eximeix els responsables de l'enfocament de risc.

L'RGPD no fixa unes mesures de seguretat únicament en consonància amb la sensibilitat de les dades utilitzades en un determinat tractament. La VISIÓ DEL RISC permet als responsables assignar mesures de seguretat de manera dinàmica en funció de les característiques i el context de cada tractament.

Quan l'RGPD es refereix a les mesures de seguretat dels tractaments de dades personals, es refereix tant a les obligacions del responsable com a les de l'ENCARREGAT O SUBENCARREGAT del tractament. Tant l'encarregat del tractament com el responsable del tractament han de tenir en compte l'establiment de

mesures tècniques i organitzatives que permetin garantir la seguretat de les dades personals.

3.5.4. El responsable de seguretat

Una figura clau en l'aplicació de les mesures de seguretat és el responsable de seguretat en les organitzacions. Se l'ha de designar dins una organització pel nomenament corresponent, el qual ha de ser conegut per tot el personal. El seu paper és determinar les decisions per satisfer els REQUISITS DE SEGURETAT de la informació i els serveis (article 10, Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, d'ara endavant ENS). Per tant, el paper del responsable de seguretat és diferent del que s'assigna al delegat de Protecció de Dades (DPD): el responsable de seguretat decideix sobre les mesures de seguretat, mentre que el paper del DPD està orientat a assessorar el responsable: informar, assessorar, supervisar el compliment, cooperar amb l'autoritat de control, etc. en el que afecta els tractaments de dades personals.

3.5.5. L'Esquema Nacional de Seguretat

La disposició addicional primera sobre mesures de seguretat en l'àmbit del sector públic de la LOPDGDD remet amb caràcter general a l'Esquema Nacional de Seguretat, que es converteix, per tant, en l'estàndard de seguretat de tot el sector públic:

> Disposició addicional primera. Mesures de seguretat en l'àmbit del sector públic.
> 1. L'Esquema Nacional de Seguretat ha d'incloure les mesures que s'han d'implantar en el cas de tractament de dades personals per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, adaptant els criteris de determinació del risc en el tractament de les dades al que estableix l'article 32 del Reglament (UE) 2016/679.
> 2. Els responsables enumerats en l'article 77.1 d'aquesta Llei orgànica han d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguin de les previstes en l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents a les empreses o fundacions vinculades als mateixos subjectes al dret privat.
> En els casos en què un tercer presti un servei en règim de concessió, comanda de gestió o contracte, les mesures de seguretat s'han de correspondre amb les de l'Administració pública d'origen i s'han d'ajustar a l'Esquema Nacional de Seguretat.

L'article 17.3 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, estableix en relació amb l'arxivament de documents que «els mitjans o suports en què s'emmagatzemin documents han de comptar amb mesures de seguretat, d'acord amb el que preveu l'Esquema Nacional de Seguretat, que garanteixin la integritat, l'autenticitat, la confidencialitat, la qualitat, la protecció i la conservació dels documents emmagatzemats. En particular, han d'assegurar la identificació dels usuaris i el control d'accessos, així com el compliment de les garanties previstes en la legislació de protecció de dades». Aquesta consideració suposa que el que preveu l'ENS és aplicable a qualsevol informació de les administracions públiques sense distinció del suport en què es trobi. D'altra banda, afegeix a la

seguretat de la informació la dimensió o característica de la TRAÇABILITAT**,** que en termes pràctics podria dir-se que és el factor de la seguretat que permet identificar unívocament les persones o els processos que accedeixen a la informació i les accions que han fet.

Per la seva banda, l'ENS en l'article 1 estableix que està constituït pels «principis bàsics i els requisits mínims per a una protecció adequada de la informació», que «serà aplicat per les administracions públiques per assegurar l'ACCÉS, LA INTEGRITAT, LA DISPONIBILITAT, L'AUTENTICITAT, LA CONFIDENCIALITAT, LA TRAÇABILITAT I LA CONSERVACIÓ DE LES DADES, LES INFORMACIONS I ELS SERVEIS utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències». L'aplicació d'aquesta norma es refereix a qualsevol informació en poder de les administracions públiques sense diferenciar-ne el contingut, tant si està constituïda per dades personals com per qualsevol altra informació.

3.6. Enfocament i anàlisi del risc

3.6.1. Introducció

L'enfocament de riscs de l'RGPD té una utilitat major que la que es refereix a la determinació de les mesures o controls de seguretat, però abans d'entrar en aquest detall és necessari fer una primera aproximació sobre alguns conceptes relacionats amb el risc.

El risc és un element amb què convivim habitualment. Qualsevol activitat que feim té implícit un risc. Les modalitats del risc són tan variades com la nostra pròpia activitat. Alguns dels riscs que habitualment s'analitzen són: de negoci, laborals, corporatius, de salut, mediambientals, riscs per a la seguretat de la informació, etc. A aquesta varietat de riscs es podria afegir un nou vessant: els RISCS PER ALS DRETS I LES LLIBERTATS DE LES PERSONES derivats dels tractaments de dades personals.

> Alguns dels riscs per als drets i les llibertats de les persones que podrien estar implícits en els tractaments de dades personals i que posa de manifest el considerant 75 de l'RGPD són: danys i perjudicis físics, discriminació, usurpació d'identitat, reputació, confidencialitat i perjudici social. Aquesta seria una mostra inicial dels riscs dels tractaments de dades per als drets i les llibertats de les persones. Caldria tenir en compte que el mateix risc no tindria les mateixes conseqüències en els drets i les llibertats de totes les persones. Per exemple, l'aïllament social en un menor podria tenir unes conseqüències diferents de les que es podrien produir en un ancià. En el cas del menor, aquest risc d'aïllament social o discriminació podria condicionar el seu desenvolupament com a persona, mentre que, en el cas de l'ancià o adult, encara que inicialment l'impacte és el mateix, les conseqüències per al seu desenvolupament com a persona són més limitades que en el cas d'un menor.

Aquest el nou enfocament de riscs que aporta l'RGPD no avalua les conseqüències que podria tenir un risc per al meu negoci, la meva salut, la meva informació com a responsable, etc. Es tracta d'avaluar el risc que té un tractament de dades per a un tercer, els riscs o les conseqüències que podria tenir un tractament de dades que no es dugui a terme d'acord amb el que

preveu l'RGPD per als mateixos interessats.

> Per exemple, si no garantesc la confidencialitat dels expedients mèdics i es produeix una vulneració del deure de secret, aquesta circumstància podria causar conseqüències negatives per a mi com a responsable, però les conseqüències per a les persones les dades de les quals hagin estat revelades i l'impacte en les seves vides podrien tenir conseqüències impredictibles. Imaginem el que podria suposar per a una persona que públicament fossin conegudes les seves limitacions cognitives: potser limitaríem la seva llibertat per trobar una feina o per relacionar-se amb altres persones perquè podria estar exposada a un aïllament social amb conseqüències poc afavoridores per exercir els seus drets i llibertats com a persona.

Quan parlam de riscs sempre hem de tenir en compte tres conceptes bàsics: el que protegim (L'ACTIU), allò contra el qual pretenem protegir l'actiu (L'AMENAÇA) i el que pretenem evitar (L'IMPACTE). Les amenaces freqüents per a la seguretat de la informació poden ser naturals, fallades d'infraestructura, errors humans, vulnerabilitats davant atacs, falta de formació i conscienciació de les persones, etc.

D'altra banda, LA QUANTIFICACIÓ DEL RISC és el resultat de multiplicar l'impacte que tindria una amenaça per la probabilitat que aquesta amenaça arribi a materialitzar-se:

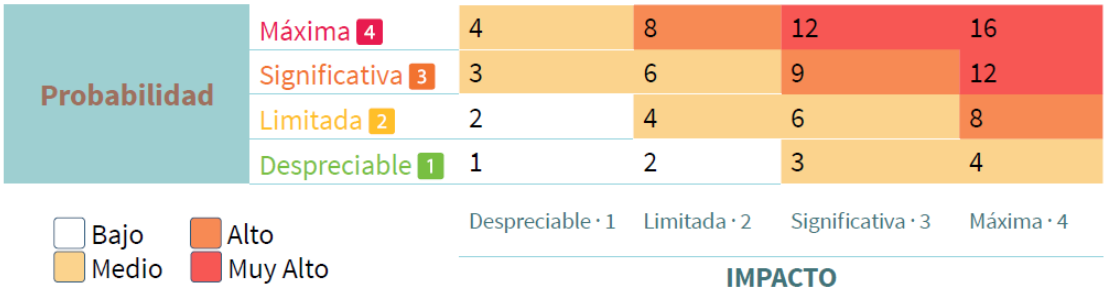
RISC = IMPACTE X PROBABILITAT

> Per exemple, quan l'impacte és molt alt i la probabilitat que una amenaça es materialitzi també és alta, tindrem un nivell de risc molt alt. En definitiva, manejam una escala amb uns valors que són específics en cada organització. La importància de l'impacte té en compte dos tipus de danys: el dany sobre els béns materials o tangibles i el dany sobre els béns intangibles. Per exemple, la falta de mesures de seguretat podria donar lloc a la pèrdua de dades personals en una empresa. Aquesta pèrdua repercutiria sobre el negoci generant pèrdues materials. Sovint pot succeir que es produeixi també la pèrdua de clients o pèrdua de negoci, ja que aquesta possible negligència implicaria una mala imatge per a l'entitat i possiblement els clients cercarien una alternativa menys negligent o amb majors garanties per a les seves dades personals. A la possible llista de danys intangibles seria necessari afegir també la llista de danys o conseqüències per als drets i les llibertats de les persones afectades per aquesta possible negligència d'un responsable.

Sovint el risc es mesura amb valors numèrics (VALORACIÓ QUANTITATIVA), però també és possible utilitzar una escala més comprensible amb valors del tipus: escàs o menyspreable, mitjà o limitat, alt o significatiu, no admissible o màxim[4]. Són escales de referència amb valors amb què mesurar el risc. Aquesta valoració dels riscs ens permet passar d'una referència abstracta i de vegades subjectiva del risc a un valor concret. En el gràfic següent es mostra un mapa de calor en què, partint de quatre nivells, es podria dur a terme la valoració quantitativa/qualitativa dels riscs. Tenint en compte aquest mapa de riscs, es podria establir una política de riscs en què únicament es duguessin a terme

4 Per facilitar la tasca d'avaluació del risc en el context de l'RGPD, l'AEPD ha publicat la Guia pràctica d'anàlisi de riscs en els tractaments de dades personals subjectes a l'RGPD.

tractaments de dades amb riscs limitats per als drets i les llibertats de les persones (nivells 1 i 2 de risc), de manera que els responsables i els encarregats haurien d'aplicar mesures per reduir els riscs (gestió del risc) des de nivells superiors fins als nivells de risc prefixats en l'organització:



En aquest sentit, les activitats de tractament han de ser avaluades amb l'objectiu de determinar el risc potencial al qual estan exposades.[5]. El pas següent és analitzar per a cada activitat de tractament si comporta un risc alt, amb l'objectiu de determinar si es requereix una avaluació d'impacte relativa a la protecció de dades (vegeu l'apartat 3.8).

3.6.2. Anàlisi i gestió del risc

Analitzar el risc no serviria de res si posteriorment no es fa un esforç per evitar-lo, reduir-lo o mitigar-lo, transferir-lo o acceptar-lo. En general aquestes són les estratègies bàsiques per tractar el risc. En el millor dels casos sempre hi haurà un risc residual o llindar de risc amb què haurem de conviure. L'activitat per a la qual evitam, reduïm o mitigam el risc, el transferim o l'acceptam és la «gestió del risc».

Una anàlisi de risc és una ACTIVITAT SISTEMÀTICA per la qual es pretén identificar cadascun dels riscs implícits en una activitat determinada. Els riscs no són estàtics: evolucionen segons l'estat de la tecnologia i les situacions específiques de cada tractament de dades personals. Cada organització hauria de tenir una política de riscs corporativa o un marc en què s'identifiqui els responsables de l'anàlisi, els recursos, els processos, els actius, la metodologia necessària per analitzar els riscs, les eines necessàries, la gestió del risc, la periodicitat de les anàlisis, les mesures de seguiment, les legislacions aplicables, la formació del personal, etc.

Per poder establir el marc de referència de l'anàlisi i la gestió del risc en una organització, poden utilitzar-se NORMES I METODOLOGIES com les següents:

- Les normes ISO 31000 I 31010 són normes generals que poden servir

5 En els casos en què es determina que el tractament de dades comporta un risc escàs per als drets i les llibertats de les persones, l'AEPD ha posat a disposició dels responsables de tractaments de dades personals l'eina Facilita_RGPD, destinada a persones i entitats que fan tractaments de dades personals que, a priori, implicarien un nivell de risc escàs per als drets i les llibertats dels interessats les dades dels quals tracten, tenint en compte que qualsevol tractament comporta un cert nivell de risc.

d'ajuda per configurar el marc de referència per analitzar riscs en general.

- La norma ISO 27005 pot utilitzar-se com a marc per analitzar riscs per a la seguretat de la informació.

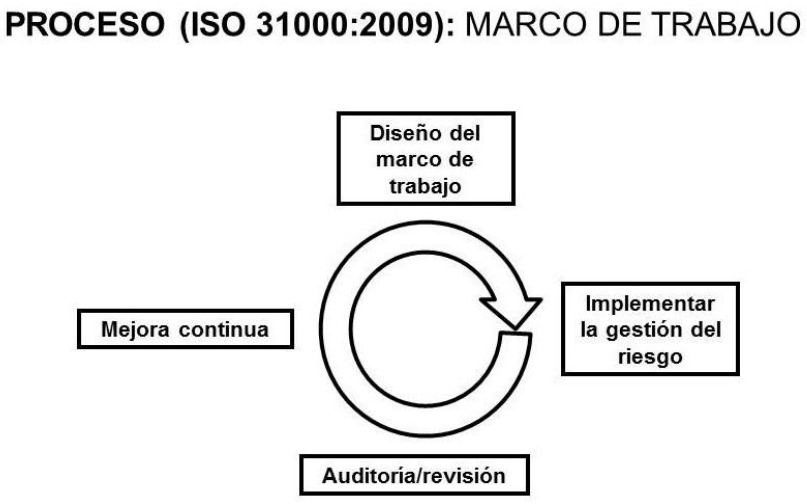
- MAGERIT és la metodologia d'anàlisi i gestió de riscs elaborada pel Consell Superior d'Administració Electrònica.

A tall d'exemple, la norma ISO 31000 defineix el procés de l'anàlisi i la gestió de riscs en quatre fases:

- Disseny i definició del marc de treball
- Implementació i gestió del risc
- Verificació dels resultats mitjançant processos d'auditoria
- Millora del marc inicial del treball La proposta d'aquesta norma, similar a qualsevol metodologia d'anàlisi i gestió del risc, es basa en un sistema de millora contínua de la qualitat.

Aquest sistema en permanent evolució tècnicament es coneix com a cicle PDCA o cicle de Deming: En altres termes podem dir que el risc és canviant segons l'entorn (marc físic, tecnològic, intervenció humana, etc.) i l'adequació de les mesures per pal·liar riscs també ha de ser canviant i en permanent adequació i revisió.

En altres paraules, podem
tecnològic, intervenció hu
riscs també ha de canvia
qual es revisen les mesur
mecanisme bàsic i neces
seguretat dels tractamen
persones.



Ciclo PDCA (Plan Do Check Act) o ciclo de Deming

3.7. Notificacions de viola

La NOTIFICACIÓ DE LES VIOLA
de l'encarregat del tracta
articles 33 i 34 de l'RGPD.
del responsable a l'Autoritat de Control i de l'encarregat al responsable, mentre que l'article 34 es refereix a les obligacions de notificació a l'interessat.

Però el que subjau a aquesta obligació de notificació és una obligació més àmplia per al responsable. Implícitament, es demana al responsable que implementi un procediment de gestió d'incidents de seguretat que afectin dades de caràcter personal.

En primer lloc, és necessari definir què és una violació de la seguretat i, per a això, és necessari remetre'ns a l'article 4, titulat Definicions, que en l'apartat 12 es defineix aquest concepte:

> És qualsevol violació de la seguretat que «ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades».

En cas que l'encarregat del tractament pateixi una violació de seguretat, l'ha de notificar sense dilació al responsable. L'RGPD no indica ni el format d'aquesta notificació ni el termini màxim perquè es faci aquesta notificació, ja que el termini establert per al responsable es fixa a partir del coneixement de la violació de seguretat. Per tant, el responsable ha de fixar les obligacions de notificació de l'encarregat, de tal manera que li permeti complir els requisits que a aquest responsable sí que obliga l'RGPD, en particular, amb relació a les dades que és necessari notificar a tercers.

El responsable ha de notificar la violació de la seguretat, sempre que existeixi risc per als drets i les llibertats de les persones físiques, risc que ha de ser avaluat pel responsable.

És necessari tenir en compte el que estableix el considerant 85, que estableix un cas específic sobre l'excepció d'informar les autoritats de control: tenint en compte el principi de responsabilitat proactiva, en cas que el responsable pugui demostrar la improbabilitat que la violació de la seguretat de les dades personals comporti un risc per als drets i les llibertats de les persones físiques.

El responsable ha de notificar la violació de seguretat a l'autoritat competent i els interessats, que en el primer cas, amb relació a les administracions públiques, i sens perjudici del que estableix la normativa nacional amb relació a les competències de les autoritats autonòmiques de protecció de dades, és l'Agència Espanyola de Protecció de Dades.

La notificació als interessats ha de fer-se en estreta cooperació amb l'autoritat de control, seguint les seves orientacions o les d'altres autoritats competents, com les autoritats policials.

L'RGPD estableix una sèrie d'excepcions a la necessitat de comunicar la violació als interessats, quan:

- El responsable del tractament ha adoptat mesures de protecció tècniques i organitzatives apropiades i aquestes mesures s'han aplicat a les dades personals afectades per la violació de la seguretat, en particular les que fan inintel·ligibles les dades personals per a qualsevol persona que no està autoritzada a accedir-hi, com pot ser el cas de les dades xifrades.

- El responsable ha pres mesures ulteriors que garanteixen que ja no

existeix la probabilitat que es materialitzi el risc alt per als drets i les llibertats de l'interessat.

- El fet que aquesta comunicació suposi un esforç desproporcionat. En aquest cas, s'optarà en el seu lloc per una comunicació pública o una mesura semblant per la qual se n'informi de manera igualment efectiva els interessats.

Cal tenir en compte que la decisió del responsable de no notificar els interessats pot ser revocada per l'Autoritat de Control, la qual pot exigir que aquesta notificació s'executi.

La notificació de la violació a l'autoritat de control s'ha de produir abans de 72 hores, és a dir, durant els tres dies següents al coneixement pel responsable de l'existència de la violació. És a dir, fins que no existeixi evidència de coneixement pel responsable no s'inicia el còmput dels terminis. Però la norma deixa oberta la possibilitat d'una notificació més enllà de les 72 hores sense establir cap condició o restricció, només l'obligació d'adjuntar a la notificació una justificació del perquè d'aquesta dilació.

La comunicació de la violació a l'Autoritat de Control va més enllà de la mera indicació que s'ha produït la violació. Al contrari, l'RGPD detalla un conjunt de dades que és obligat incorporar-hi, com a mínim:

- Una descripció de la naturalesa de la violació de la seguretat de les dades personals. Per descriure la naturalesa cal incloure-hi, sempre que sigui possible:
  - Les categories d'interessats afectats, és a dir, quin tipus de persones han estat afectades per la violació. Aquesta classificació pot atendre la vulnerabilitat dels interessats, com menors o discapacitats, la relació amb l'empresa, com clients o empleats, o la rellevància dels subjectes, com podrien ser jutges o policies.
  - El nombre aproximat d'interessats afectats. És recomanable desglossar aquest nombre per a les categories anteriors.
  - Les categories de dades compromeses. Això significa que no és necessària una descripció exhaustiva dels diferents camps de dades, sense descriure-les de manera genèrica, tenint especial atenció d'assenyalar les dades que són especialment sensibles.
  - El nombre aproximat de registres de dades personals afectats.
- Comunicar el nom i les dades de contacte del delegat de protecció de dades o, si escau, d'un altre punt de contacte en què pugui obtenir-se'n més informació. Aquestes opcions no són exclusives.
- Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.
- Descriure les mesures adoptades o proposades pel responsable del tractament per posar remei a la violació de la seguretat de les dades personals. Això ha d'incloure, si escau, les mesures adoptades per mitigar els possibles efectes negatius

Hem de DESTACAR QUE AQUESTA INFORMACIÓ ÉS UN MÍNIM, NO UN MÀXIM. És important assenyalar que en la redacció de l'RGPD es considera de manera implícita que és recomanable afegir-hi qualsevol informació addicional que permeti a l'Autoritat de Control prendre accions presents futurs per garantir la protecció dels drets dels interessats, i que l'AEPD i els seus funcionaris tenen l'obligació

de guardar secret de la informació rebuda en el marc de les seves actuacions.

Gran part d'aquesta informació no es podrà proporcionar en aquest termini de 72 hores, per la qual cosa l'RGPD estableix la prioritat de fer una comunicació a l'Autoritat en aquest termini, encara que sigui incompleta, i l'obligació de mantenir informada a l'Autoritat de les noves dades relatives a la violació que vagin apareixent.

La notificació als interessats no té un termini temporal establert en l'RGPD. Només s'hi assenyala que ha de produir-se com més aviat millor, tenint en compte, en particular, la naturalesa i gravetat de la violació de la seguretat de les dades personals i les conseqüències i els efectes adversos que pot tenir per a l'interessat.

> S'han de comunicar a l'interessat tant el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en què pugui obtenir-se més informació de les possibles conseqüències de la violació de la seguretat de les dades personals, com les mesures adoptades o proposades pel responsable del tractament per posar remei a la violació de la seguretat de les dades personals, incloent-hi, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius. Aquesta informació ha de traslladar-se a l'interessat amb un llenguatge clar i senzill, per la qual cosa ha d'adequar-se a la categoria del subjecte i la seva capacitat per entendre la informació que se li subministra. L'objectiu d'aquesta notificació és que l'interessat pugui conèixer les implicacions del que ha passat i quines mesures personals pot adoptar per protegir els seus drets. Per tant, ha de ser una informació eminentment pràctica.

El responsable ha d'implementar un procediment documentat de gestió de les violacions de seguretat. Aquest procediment ha de registrar tots els fets relacionats amb la violació. A més, cal incloure-hi una avaluació de si s'hi ha aplicat tota la protecció tecnològica adequada i s'han pres les mesures organitzatives oportunes per detectar la violació de seguretat. Cal registrar els efectes produïts per la violació, que poden anar més enllà del compromís de les dades de caràcter personal i poden ser relatius a la prestació de determinats serveis, per exemple. Al seu torn, s'han de documentar les mesures correctives tant per minimitzar els efectes de la violació com evitar que torni a produir-se.

Tota aquesta informació ha de posar-se a disposició de les autoritats de control en la seva missió de verificar, si escau, la diligència del responsable en el tractament de les dades i en la gestió de la violació de seguretat.

3.8. Avaluacions d'impacte de protecció de dades

El risc en l'RGPD té diverses perspectives: la primera és garantir les mesures de seguretat de conformitat en cada moment amb l'estat de la tecnologia i les condicions específiques dels tractaments de dades personals. Les avaluacions d'impacte poden definir-se com una anàlisi de riscs d'un producte, servei o sistema que encara no existeix i es vincula als principis de protecció de dades des del disseny i protecció de dades per defecte.

L'RGPD recull les avaluacions d'impacte en l'article 35:

> 1. Quan sigui probable que un tipus de tractament, en particular si utilitza noves tecnologies, per la seva naturalesa, abast, context o fins, comporti un risc alt per als drets i les llibertats de les persones físiques, el responsable del tractament ha de fer, abans del tractament, una avaluació de l'impacte de les operacions de tractament en la protecció de dades personals. Una única avaluació pot abordar una sèrie d'operacions de tractament similars que comportin riscs alts similars.
> 2. El responsable del tractament ha de recollir l'assessorament del delegat de protecció de dades, si ha estat nomenat, en fer l'avaluació d'impacte relativa a la protecció de dades.
> 3. És necessària l'avaluació d'impacte relativa a la protecció de les dades a què es refereix l'apartat 1 en cas de:
> *a)* avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques que es basa en un tractament automatitzat, com l'elaboració de perfils, i sobre la base de la qual es prenen decisions que produeixen efectes jurídics per a les persones físiques o que les afecten significativament de manera similar;
> *b)* tractament a gran escala de les categories especials de dades a les quals es refereix l'article 9, apartat 1, o de les dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10, o
> *c)* observació sistemàtica a gran escala d'una zona d'accés públic.
> 4. L'autoritat de control ha d'establir i publicar una llista dels tipus d'operacions de tractament que requereixin una avaluació d'impacte relativa a la protecció de dades de conformitat amb l'apartat 1. L'autoritat de control ha de comunicar aquestes llistes al Comitè al qual es refereix l'article 68.
> 5. L'autoritat de control també pot establir i publicar la llista dels tipus de tractament que no requereixen avaluacions d'impacte relatives a la protecció de dades. L'autoritat de control ha de comunicar aquestes llistes al Comitè.
> 6. Abans d'elaborar les llistes a les quals es refereixen els apartats 4 i 5, l'autoritat de control competent ha d'aplicar el mecanisme de coherència establert en l'article 63 si aquestes llistes inclouen activitats de tractament que guarden relació amb l'oferta de béns o serveis a interessats o amb l'observació del comportament d'aquests interessats en diversos estats membres, o activitats de tractament que puguin afectar substancialment la lliure circulació de dades personals en la Unió.
> 7. L'avaluació ha d'incloure com a mínim:
> *a)* una descripció sistemàtica de les operacions de tractament previstes i dels fins del tractament, incloent-hi, quan escaigui, l'interès legítim perseguit pel responsable del tractament;
> *b)* una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte a la seva finalitat;
> *c)* una avaluació dels riscs per als drets i llibertats dels interessats a què es refereix l'apartat 1, i
> *d)* les mesures previstes per afrontar els riscs, incloent-hi garanties, mesures de seguretat i mecanismes que garanteixin la protecció de dades personals, i demostrar la conformitat amb aquest Reglament, tenint en compte els drets i els interessos legítims dels interessats i d'altres persones afectades.
> 8. El compliment dels codis de conducta aprovats als quals es refereix l'article 40 per part dels responsables o encarregats corresponents es s'ha de tenir degudament en compte en avaluar les repercussions de les operacions de tractament fetes per aquests responsables o encarregats, en particular a l'efecte de l'avaluació d'impacte relativa a la protecció de dades.
> 9. Quan escaigui, el responsable recollirà l'opinió dels interessats o dels seus representants en relació amb el tractament previst, sens perjudici de la protecció d'interessos públics o comercials o de la seguretat de les operacions de tractament.
> 10. Quan el tractament de conformitat amb l'article 6, apartat 1, lletres *c)* o *e)* tengui la base jurídica en el dret de la Unió o en el dret de l'Estat membre que s'apliqui al responsable del tractament, aquest dret reguli l'operació específica de tractament o

conjunt d'operacions en qüestió, i ja s'hagi realitzat una avaluació d'impacte relativa a la protecció de dades com a part d'una avaluació d'impacte general en el context de l'adopció d'aquesta base jurídica, els apartats 1-7 no seran aplicables excepte si els estats membres consideren necessari avaluar prèviament les activitats de tractament.
11. En cas necessari, el responsable ha d'examinar si el tractament és conforme amb l'avaluació d'impacte relativa a la protecció de dades, almenys quan existeixi un canvi del risc que representin les operacions de tractament.

El grup de l'article 29, en el document Directrius sobre les avaluacions d'impacte en la protecció de dades introdueix criteris que poden evidenciar un risc elevat inherent a les activitats de tractament i que s'han d'avaluar i poden determinar la necessitat de fer-les.

Així, podem esmentar, entre altres:

- Monitoratge sistemàtic (procediment utilitzat per observar o controlar els interessats, incloent-hi les dades recopilades a través de xarxes o un sistema de control d'una àrea d'accés públic);

- Dades relatives a les persones vulnerables (els subjectes de dades vulnerables poden incloure menors, segments més vulnerables de la població que requereixen protecció especial: persones amb malalties mentals, sol·licitants d'asil o ancians, pacients).

- Ús innovador o aplicació de solucions tecnològiques o organitzatives noves (activitats de tractament fetes usant tecnologia innovadora que pugui implicar formes noves de recopilació i ús de dades, possiblement amb un risc alt per als drets i llibertats de les persones –per exemple, combinació de l'ús de l'empremta dactilar i el reconeixement facial per millorar el control d'accés físic).

En execució de les habilitacions de l'RGPD, l'AEPD ha publicat llistes de criteris: «positiva», que li permet determinar quan fer una avaluació d'impacte relativa a la protecció de dades, i «negativa», que permet excloure aquesta obligació.

Llista positiva

Llista orientativa de tipus de tractaments que requereixen una avaluació d'impacte relativa a la protecció de dades segons l'article 35.4 de l'RGPD
En el moment d'analitzar tractaments de dades serà necessari fer una avaluació d'impacte relativa a la protecció de dades en la majoria dels casos en què aquest tractament compleixi dos o més criteris de la llista exposada a continuació, llevat que el tractament es trobi en la llista de tractaments que no requereixen avaluació d'impacte relativa a la protecció de dades a què es refereix en article 35.5 de l'RGPD. Com més criteris reuneixi el tractament en qüestió, majors seran el risc que comporta aquest tractament i la certesa de la necessitat de fer una avaluació d'impacte relativa a la protecció de dades.
Aquesta llista es basa en els criteris establerts pel Grup de Treball de l'Article 29 en la guia WP248 «Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (AIPD) i per determinar si el tractament "entranya probablement un alt risc" a l'efecte de l'RGPD», els complementa i s'ha d'entendre com una llista no exhaustiva:

1. Tractaments que impliquen elaboració de perfils o valoració de subjectes, incloent-hi la recollida de dades del subjecte en múltiples àmbits de la seva vida (acompliment a la feina, personalitat i comportament), que cobreixin diversos aspectes de la seva personalitat o sobre els seus hàbits.
2. Tractaments que impliquen la presa de decisions automatitzades o que contribueixen en gran mesura a la presa d'aquestes decisions, incloent-hi qualsevol tipus de decisió que impedeixi a un interessat exercir un dret, accedir a un bé o un servei o formar part d'un contracte.
3. Tractaments que impliquin l'observació, la monitorització, la supervisió, la geolocalització o el control de l'interessat de manera sistemàtica i exhaustiva, incloent-hi la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic, així com el processament d'identificadors únics que permetin la identificació d'usuaris de serveis de la societat de la informació com poden ser els serveis web, TV interactiva, aplicacions mòbils, etc.
4. Tractaments que impliquen l'ús de categories especials de dades a què es refereix l'article 9.1 de l'RGPD, dades relatives a condemnes o infraccions penals a les quals es refereix l'article 10 de l'RGPD o dades que permeten determinar la situació financera o de solvència patrimonial o deduir informació sobre les persones relacionada amb categories especials de dades.
5. Tractaments que impliquen l'ús de dades biomètriques amb el propòsit d'identificar de manera única una persona física.
6. Tractaments que impliquen l'ús de dades genètiques per a qualsevol fi.
7. Tractaments que impliquen l'ús de dades a gran escala. Per determinar si un tractament es pot considerar a gran escala, es consideraran els criteris establerts en la guia WP243 «Directrius sobre els delegats de protecció de dades (DPD)» del Grup de Treball de l'Article 29.
8. Tractaments que impliquen l'associació, la combinació o l'enllaç de registres de bases de dades de dos o més tractaments amb finalitats diferents o per part de responsables diferents.
9. Tractaments de dades de subjectes vulnerables o en risc d'exclusió social, incloent-hi dades de menors de 14 anys, majors amb algun grau de discapacitat, discapacitats, persones que accedeixen a serveis socials i víctimes de violència de gènere, així com els seus descendents i persones que estiguin sota la seva guàrdia i custòdia.
10. Tractaments que impliquen la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, incloent-hi la utilització de tecnologies a una escala nova, amb un objectiu nou o combinades amb altres, de manera que suposin formes noves de recollida i utilització de dades amb risc per als drets i les llibertats de les persones.
11. Tractaments de dades que impedeixen als interessats exercir els seus drets, utilitzar un servei o executar un contracte, com tractaments en què les dades han estat recopilades per un responsable diferent del que les tractarà i que aplica alguna de les excepcions sobre la informació que ha de proporcionar-se als interessats segons l'article 14.5 (*b, c, d*) de l'RGPD.

Llista negativa

En la llista següent s'estableixen els tractaments exempts d'AIPD, sens perjudici d'altres obligacions que s'estableixen en l'RGPD. Per tant, no és una llista d'exempció de les obligacions que estableix la normativa de protecció de dades sobre els tractaments de dades personals.
Aquesta llista es basa en el document WP 248 i el complementa per ajudar els responsables a determinar quins tractaments no requereixen una AIPD.

1. Tractaments que es fan estrictament sota les directrius establertes o autoritzades amb anterioritat mitjançant circulars o decisions emeses per les autoritats de control, en particular l'AEPD, sempre que el tractament no s'hagi modificat d'ençà que va ser autoritzat.
2. Tractaments que es fan estrictament sota les directrius de codis de conducta aprovats per la Comissió Europea o les autoritats de control, en directrius sobre l'avaluació d'impacte relativa a la protecció de dades (AIPD) i per determinar si el tractament «entranya probablement un alt risc» a l'efecte del Reglament (UE), 2016/679, particularment l'AEPD, sempre que s'hagi fet una AIPD completa per validar el codi de conducta i el tractament s'implementa incloent-hi les mesures i les salvaguardes definides en l'AIPD.
3. Tractaments que siguin necessaris per al compliment d'una obligació legal o una missió duita a terme en interès públic o en l'exercici de poders públics conferits al responsable, sempre que en el mateix mandat legal no s'obligui a fer una AIPD, i sempre que ja s'hagi realitzat una AIPD completa.
4. Tractaments duits a terme en l'exercici de la seva tasca professional per treballadors autònoms que exerceixin de manera individual, en particular metges, professionals de la salut o advocats, sens perjudici que pugui requerir-se quan el tractament que duguin a terme compleixi, de manera significativa, dos o més criteris establerts en la llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a protecció de dades publicada per l'AEPD.
5. Tractaments obligatoris per llei i realitzats en relació amb la gestió interna del personal de les pimes amb fins de comptabilitat, gestió de recursos humans i nòmines, seguretat social i salut laboral, però mai relatius a les dades dels clients.
6. Tractaments realitzats per comunitats i subcomunitats de propietaris, tal com es defineixen en l'article 2 (*a, b i d*) de la Llei 49/1960, de propietat horitzontal.
7. Tractaments fets per col·legis professionals i associacions sense ànim de lucre per gestionar les dades personals dels seus propis associats i donants, i en l'exercici de la seva tasca, sempre que no incloguin en el tractament dades sensibles com ara les que s'estableixen en l'article 9.1 de l'RGPD i no sigui aplicable l'article 9.2 (*d*) d'aquest Reglament.

Per facilitar la realització d'aquestes avaluacions, l'AEPD ha publicat la Guia pràctica per a les avaluacions d'impacte en la protecció de dades subjectes a l'RGPD.

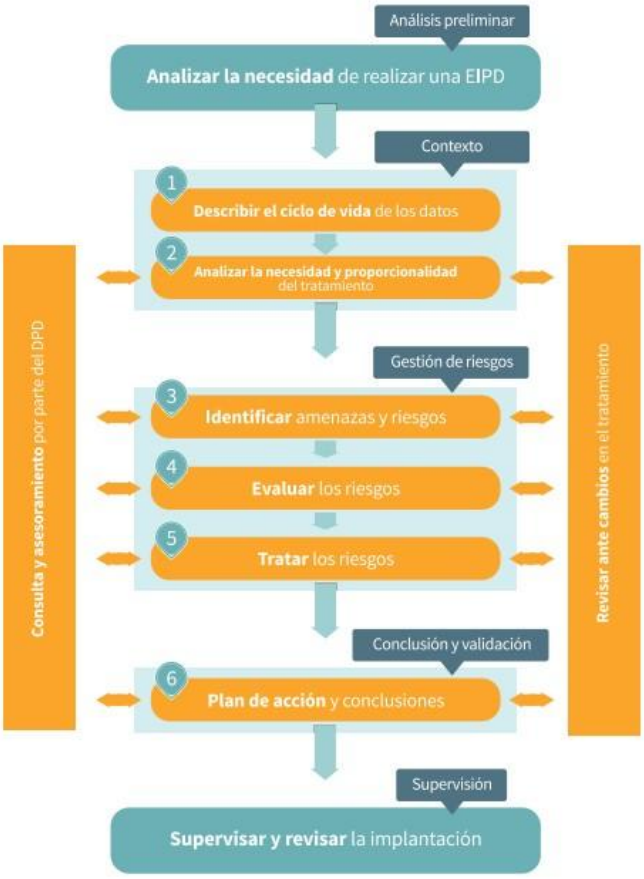
Aquestes avaluacions han de fer-se abans del tractament, per bé que el mandat de l'RGPD no s'estén a les operacions de tractament que ja estiguin en curs en el moment en què comenci a ser aplicable. Tanmateix, sí que hauria de fer-se una avaluació quan en una operació iniciada abans de l'aplicació de l'RGPD s'hagin produït canvis en els riscs que el tractament implica en relació amb el moment en què es va posar en marxa el tractament.

D'altra banda, cal assenyalar que a l'hora de fer una AIPD, s'ha de disposar d'una metodologia que consideri els requisits exigits per l'RGPD en l'article 35.7, en el

qual s'indica que com a mínim ha de ser:

- Una descripció sistemàtica de l'activitat de tractament prevista.
- Una avaluació de la necessitat i la proporcionalitat del tractament respecte a la seva finalitat.
- Una avaluació dels riscs.
- Les mesures previstes per afrontar els riscs, incloent-hi garanties, mesures de seguretat i mecanismes que garanteixin la protecció de dades personals.

L'estructura amb les diferents etapes d'una avaluació i el flux que cal seguir en l'execució podria ser la següent:



De la mateixa manera que s'ha esmentat en l'anàlisi de riscs, en les avaluacions d'impacte també és necessari tenir una política de revisió i anàlisi dels riscs continuada, duent a terme auditories periòdiques en què es posi de manifest l'eficàcia de les mesures que s'hagin adoptat per minimitzar els riscs dels tractaments i en especial els riscs per als drets i les llibertats dels interessats. En definitiva, l'enfocament de riscs implica un procés de revisió i millora contínua de les activitats de tractament.