apdcat
Autoritat Catalana de Protecció de Dades

Avaluació d'impacte relativa a la protecció de dades

Actualització: juny 2022

Col·lecció guies. Núm. 4

Generalitat de Catalunya

Índex

1. Introducció

El Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 de abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament i la lliure circulació de dades personals, en definitiva el Reglament general de protecció de dades (d'ara endavant, RGPD o Reglament), incorpora una nova obligació per als responsables de tractaments: avaluar l'impacte de les operacions de tractament en la protecció de les dades personals, quan sigui probable que el tractament comporti un risc significatiu per als drets i les llibertats de les persones.

En general, la reforma de la protecció de dades a Europa proposa un model de compliment orientat a la gestió, que superi el model previ, de caire massa formalista en alguns dels seus aspectes. De la nova regulació en destaca el fet que cal demostrar que es compleixen les obligacions, i precisament les avaluacions d'impacte relatives a la protecció de les dades de caràcter personal (d'ara endavant, AIPD) se situen en el punt de partida per demostrar una gestió responsable dels tractaments.

L'execució de les AIPD s'ha de basar en mètodes sistemàtics, a fi que resultin objectives, repetibles i comparables, i quedin documentades. Per això, els continguts d'aquesta guia tenen com a finalitat orientar en la manera d'abordar l'execució de les avaluacions d'impacte, d'acord amb el que preveu l'RGPD.

Podem classificar els riscos associats a un tractament en dos tipus: els riscos inherents al tractament (tal com ha estat dissenyat) i els riscos associats a la seguretat de les dades. L'enfocament en el risc que proposa el Reglament exigeix analitzar els riscos i, si són massa alts, reduir-los.

Quan els riscos inherents al tractament són massa alts, cal modificar el tractament; això es pot fer, per exemple, evitant de tractar algun tipus de dada especialment sensible o restringint l'accés a certs tipus de dades.

El tractament dels riscos associats a la seguretat de les dades s'ha de basar en una anàlisi del risc associat a la pèrdua de la confidencialitat, la integritat i la disponibilitat de les dades. Les metodologies d'anàlisi de riscos estàndard (per exemple, ISO i Magerit) són complexes i poden ser difícils de portar a terme per organitzacions petites. En aquesta guia proposem una metodologia alternativa, que busca simplificar l'anàlisi però sense reduir l'exhaustivitat de les mesures de control. Quan l'anàlisi de riscos suggereix que el risc és massa alt, cal aplicar controls de seguretat per reduir-lo.

2. Introducció a les AIPD

Punts clau

- Una avaluació d'impacte en protecció de dades (AIPD) és un procediment que pretén identificar i controlar els riscos associats a un tractament de dades.
- Cal fer una AIPD quan el tractament pot suposar un alt risc per als drets i les llibertats de les persones.

2.1 Què és una avaluació d'impacte?

Una avaluació d'impacte en protecció de dades (AIPD) és un procediment que busca identificar i controlar el riscos per als drets i les llibertats de les persones, associats a un tractament de dades. Les AIPD també són instruments útils en relació amb el principi de responsabilitat proactiva[1].

El Reglament estableix els drets que tenen les persones pel que fa al tractament de les seves dades (dret a la informació, etc.). Ara bé, quan es parla dels "riscos per als drets i les llibertats de les persones" no ens limitem als drets reconeguts pel Reglament, sinó a qualsevol efecte que el tractament pugui tenir sobre els drets i les llibertats fonamentals de les persones: dret a la llibertat d'expressió, a la llibertat de pensament, a la prohibició de patir discriminació, a la llibertat de consciència, a la llibertat de religió, etc.

En identificar els riscos, hem de considerar qualsevol impacte que el tractament pugui tenir sobre les persones (físic, econòmic, emocional, etc.). Alguns impactes potencials són:

- Impossibilitat d'accedir a serveis o altres oportunitats.
- Discriminació.
- Robatori de la identitat i altres fraus.
- Pèrdues econòmiques.
- Danys a la reputació.
- Danys físics.
- Pèrdua de la confidencialitat.
- Impossibilitat d'exercir algun dret.

[1] *Accountability*, en el seu terme en anglès.

Aquests impactes es poden materialitzar per dues raons principals. La primera és que el tractament, tal com està dissenyat, pugui donar lloc a aquests impactes; ja sigui pel tipus de dades que es tracten, per qui hi té accés, pel potencial efecte del tractament, etc. La segona està relacionada amb la seguretat de les dades; en particular, la pèrdua de la confidencialitat, la integritat o la disponibilitat de les dades.

Per controlar els riscos inherents al tractament, hem d'establir els controls necessaris per garantir que el tractament es fa d'acord amb l'RGPD. En particular, que és necessari i proporcionat i que s'estableixen els mecanismes necessaris perquè les persones interessades puguin exercir els seus drets.

Per controlar els riscos que afecten la seguretat de les dades, cal fer una anàlisi que permeti identificar i valorar els riscos i, després, establir les salvaguardes apropiades a les valoracions de risc.

2.2 Quan cal fer una avaluació d'impacte?

L'RGPD exigeix que el responsable del tractament executi una AIPD, quan el tractament pot comportar un risc alt per als drets i les llibertats de les persones. L'RGPD no descriu què s'entén per risc alt; es limita a donar una llista de tres casos en què l'AIPD és obligatòria[2].

Atesa la manca d'especificitat de l'RGPD, seguirem el procediment que descriu el GT29, que dona una llista de nou característiques dels tractaments que poden ser indicatives d'un risc alt (vegeu més avall). A major nombre d'aquestes característiques, més probable és que un tractament presenti un risc greu. Segons el GT29, cal fer una AIPD quan el tractament en presenta dues o més, tot i que indica que pot ser convenient fer l'AIPD fins i tot en alguns casos en què només en presenta una.

1. Avaluació o puntuació, incloses l'elaboració de perfils i prediccions.

   Especialment en relació amb el rendiment laboral, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, ubicació o moviments. Exemples:

   - Una institució financera que investiga els seus clients en una base de dades de referència de crèdit.
   - Una empresa biotecnològica que ofereix proves genètiques per avaluar i predir els riscos de patir malalties.

[2] RGPD, article 35.3.

- Una empresa que fa perfils de comportament basats en la navegació web.

2. Presa de decisions automatitzada amb efectes jurídics o que afecta de manera similar i significativa la persona física.

   Per exemple, un tractament automatitzat que pot donar lloc a exclusió o discriminació de les persones.

3. Observació sistemàtica d'una àrea d'accés públic.

   En aquest tractament, les dades es poden recollir sense que els interessats siguin conscients que s'estan recollint i de com s'usaran.

4. Dades sensibles.

   Això inclou les categories especials de dades mencionades a l'article 9 de l'RGPD:

   - Origen racial o ètnic.
   - Opinions polítiques o filosòfiques.
   - Pertinença a un sindicat.
   - Dades genètiques.
   - Dades biomètriques tractades amb la finalitat d'identificar una persona de forma exclusiva.
   - Dades relatives a la salut.
   - Dades relatives a la vida sexual o l'orientació sexual.

   També inclou:

   - Dades relatives a condemnes o delictes penals.
   - Dades que augmenten el risc per als drets i les llibertats de les persones (com ara dades de comunicacions electròniques, dades de localització i dades financeres).
   - Documents personals, correu electrònic, diaris, notes de lectors de llibres electrònics i informació personal inclosa en aplicacions de registre d'activitats vitals.

5. Tractament de dades a gran escala.
   Per determinar si un tractament és a gran escala, cal tenir en compte els factors següents:

   - El nombre de persones a les quals es refereixen les dades, ja sigui en termes absoluts o com a proporció de la població subjacent.
   - El volum o la varietat de dades.

- La durada o permanència de l'operació de tractament.
- L'extensió geogràfica de l'operació de tractament.

6. Conjunts de dades que s'han enllaçat o combinat

7. Dades relacionades amb persones vulnerables
   Això inclou totes les situacions en què es detecti un desequilibri entre la posició del responsable del tractament i l'interessat. Per exemple:

   - Tractament de dades d'empleats en relació amb la gestió de recursos humans.
   - Nens i persones grans.
   - Persones amb malalties mentals.
   - Sol·licitants d'asil.

8. Ús innovador de tecnologies

9. Tractament que en si mateix impedeix l'exercici d'un dret o l'ús d'un servei contracte
   Per exemple:

   - Tractaments fets en un espai públic que les persones vianants no poden evitar.
   - Consulta de l'historial de crèdit d'una persona usuària per part d'un banc, per decidir si li concedeix un crèdit.

Comentaris

- En versions anteriors de la guia sobre AIPD del GT29, hi apareixia un supòsit addicional: la transferència de dades fora de la UE. A la revisió 1 es va eliminar aquest supòsit.
- Segons l'article 35.4 de l'RGPD, les autoritats de protecció de dades han de publicar una llista de tractaments per als quals cal fer l'AIPD. Hi ha una tendència general a adoptar la proposta del GT29. Aquest és el cas de l'autoritat catalana (APDCAT) i de l'espanyola (AEPD).

Exemples

- Un hospital que tracta dades sanitàries de pacients.
  Criteris que són d'aplicació:

  - Dades sensibles.
  - Tractament a gran escala.

  - Dades relatives a persones vulnerables

- Ús de càmeres per controlar el comportament de les persones conductores. Es preveu l'ús d'un sistema intel·ligent per seleccionar cotxes i reconèixer matrícules.
  Criteris que són d'aplicació:

  - Observació sistemàtica.
  - Ús innovador de tecnologies.

- Una empresa que observa sistemàticament les activitats dels seu personal, del lloc de treball, de l'activitat a internet, etc.
  Criteris que són d'aplicació:

  - Observació sistemàtica.
  - Dades relatives a persones vulnerables.

- Recollida de dades públiques per elaborar perfils.
  Criteris que són d'aplicació:

  - Avaluació o puntuació.
  - Tractament a gran escala.
  - Conjunts de dades que s'han enllaçat o combinat.

Independentment del risc que pugui tenir un tractament, en els casos següents no cal fer una AIPD:

- Quan la naturalesa, l'abast, el context i les finalitats del tractament són molt semblants a un altre tractament per al qual ja s'ha fet una AIPD.
- Quan un tractament té una base jurídica en el dret de la UE o d'un estat membre, i ja s'ha fet una AIPD en el moment d'adoptar aquesta base jurídica.
- Quan el tractament està inclòs en una llista de tractaments (publicada per l'autoritat competent) que no requereixen una AIPD. Hores d'ara, ni l'APDCAT ni l'AEPD han publicat aquesta llista.

Comentaris

- No cal fer una AIPD si l'RGPD no és d'aplicació al tractament.
- L'RGPD és d'aplicació al tractament de dades personals fet per una empresa o organització situada a la UE o en un lloc on el dret comunitari sigui d'aplicació, o per una empresa o organització situada fora de la UE, si aquesta tracta dades de persones residents a la UE per a activitats relacionades amb l'oferta de béns o serveis i per controlar el comportament.

Les operacions de tractament poden evolucionar ràpidament, cosa que pot afectar els riscos i la necessitat d'executar una AIPD, com també els canvis en el context del tractament. Per exemple, canvis en l'estructura organitzativa del responsable del tractament, o canvis socials que incrementen el risc o la percepció que en tenim. Un exemple del darrer cas seria quan la societat pren consciència que hi ha un grup de persones que és vulnerable a patir discriminació.

Si l'AIPD és obligatòria i no s'executa, els tractaments queden exposats a uns riscos no detectats. No s'hauran analitzat ni valorat i, en conseqüència, no s'hauran adoptat les mesures que haurien de servir per mitigar els efectes negatius que les operacions de tractament poden tenir per als drets i les llibertats de les persones. Segons l'article 83 de l'RGPD, no fer una AIPD que és necessària és una infracció sancionable.

2.3 Com es fa una AIPD?

2.3.1 En quin moment cal fer AIPD?

Cal fer l'AIPD tan aviat com sigui possible. En particular, per a nous tractaments cal fer- la abans de començar a tractar les dades. Això està d'acord amb la protecció de dades per disseny i per defecte, i permet fer ús de l'AIPD com a eina per ajudar a la presa de decisions en el disseny del tractament.

En el cas d'una operació de tractament que ja està en marxa, convé fer una AIPD tan aviat com es detecti un risc greu per als drets i les llibertats de les persones. Convé remarcar que les AIPD no són una tasca puntual, sinó que impliquen un procés continu de reavaluació. En particular, cal reavaluar la necessitat de fer una AIPD quan es produeixen canvis significatius en l'operació de tractament o en el seu context (organitzatiu o social).

2.3.2 Qui intervé en una AIPD?

El responsable del tractament és l'actor principal, atès que és qui té la responsabilitat que l'AIPD s'executi. Això no treu que el responsable del tractament pugui delegar l'AIPD però, en qualsevol cas, és qui en té la responsabilitat última.

L'encarregat del tractament, si n'hi ha, ha de donar suport al responsable a l'hora de fer l'AIPD.

El responsable del tractament ha de buscar el consell del delegat de protecció de dades (DPD). Aquest consell i les decisions que prengui han de quedar documentades a l'AIPD. En

particular, el responsable del tractament ha de demanar opinió al DPD en els aspectes següents:

- Determinar si cal fer una AIPD.
- La metodologia a usar en l'AIPD.
- Determinar si convé fer l'AIPD internament o si és millor externalitzar-la.
- Les mesures adoptades per protegir els drets i les llibertats de les persones.
- Determinar si l'AIPD s'ha fet correctament i si les conclusions satisfan els requeriments de protecció de dades.

El responsable del tractament ha de buscar l'opinió de les persones interessades sobre l'operació de tractament, quan això es consideri apropiat. Si no es considera apropiat, cal documentar el perquè; per exemple, per què buscar aquesta opinió té un cost desproporcionat, és impracticable o pot posar en risc la confidencialitat del pla de negoci.

L'opinió de les persones interessades es pot recollir de diferents maneres: enquestes, consulta a representants del personal, etc. En qualsevol cas, cal que el responsable del tractament tingui base legal per tractar qualsevol dada personal que es generi en recollir aquestes opinions.

A banda dels actors anteriors, pot ser necessari que hi concorrin tot un seguit d'agents interns o externs a l'organització, com poden ser unitats o àrees específiques, persones expertes independents, responsables de seguretat, etc.

2.3.3 Quin és el contingut mínim d'una AIPD?

El resultat final d'una avaluació d'impacte no deixa de ser un informe, o un conjunt de documentació, que recull les característiques del tractament avaluat i les decisions preses per mitigar-ne els riscos, d'acord amb la seva identificació, anàlisi, valoració. En base a aquests riscos, també es valora la necessitat i la proporcionalitat de les operacions de tractament.

L'RGPD fixa el següent contingut mínim per a una AIPD:

- Descripció de les operacions de tractament.
- Avaluació de la necessitat i de la proporcionalitat del tractament.
- Avaluació del risc per als drets i les llibertats de les persones.
- Mesures adoptades per mitigar els riscos.

2.3.4 Quines són les fases d'una AIPD?

La realització d'una AIPD ha de seguir un procés sistemàtic, objectiu, repetible i comparable. En aquesta guia, proposem una metodologia estructurada en sis fases:

1. Necessitat de fer una AIPD. Tot i que aquesta part hauria de ser una anàlisi prèvia a l'AIPD, perquè quedi constància que s'ha analitzat la necessitat de fer- la, serà la primera secció a la plantilla d'AIPD que proposem. Aquesta part és especialment interessant quan es conclou que no cal fer l'AIPD.

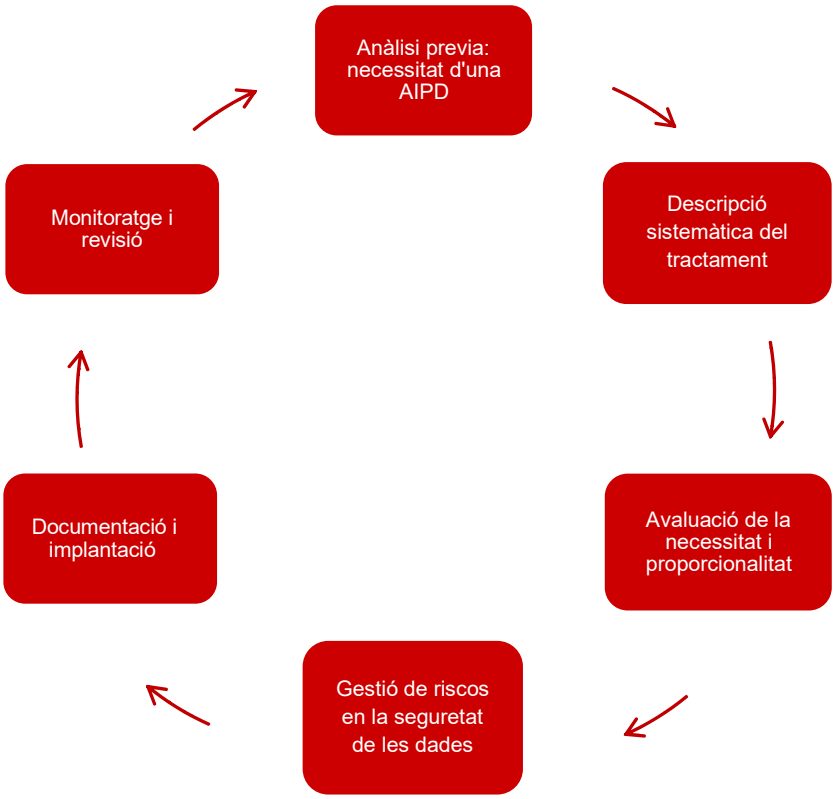
2. Descripció sistemàtica del tractament. La descripció del tractament i el context en què té lloc és essencial per determinar els riscos que comporta.

3. Avaluació de la necessitat i la proporcionalitat del tractament. Qualsevol tractament de dades té una finalitat. Cal dissenyar el tractament que sigui menys intrusiu per assolir aquesta finalitat (necessitat) i cal que el benefici del tractament sigui superior als potencials perjudicis (proporcionalitat).

4. Gestió de riscos en la seguretat de les dades. S'avalua el risc sobre els drets i les llibertats de les persones que pot tenir la vulneració de la seguretat de les dades. El risc es deriva de l'impacte i de la probabilitat que la vulneració es produeixi. Com més alt sigui el risc, més exhaustius han de ser els controls per reduir-lo.

5. Documentació i implantació. El resultat d'una AIPD és un document que descriu les anàlisis fetes en els punts anteriors. Les mesures adoptades per salvaguardar els drets i les llibertats de les persones s'han d'implementar al sistema de tractament.

6. Monitoratge i revisió. L'AIPD no s'acaba quan es completa la documentació i la implantació. Les AIPD necessiten un procés de monitoratge per detectar canvis en els riscos (ja sigui a conseqüència de canvis en el tractament o en la percepció de risc de la societat), que poden requerir que es revisi l'AIPD o, fins i tot, que es refaci.



2.4 Què cal fer si l'AIPD conclou que el risc és alt?

Segons l'article 36, si l'AIPD conclou que el tractament comporta un alt risc, el responsable del tractament ha de consultar l'autoritat de control abans d'iniciar el tractament.

Un cop l'autoritat de control té tota la documentació necessària, ha de respondre per escrit en un termini de vuit setmanes. Aquest termini es pot ampliar sis setmanes més, d'acord amb la complexitat del tractament.

En el context d'una consulta prèvia, l'autoritat de protecció de dades pot utilitzar qualsevol dels poders recollits a l'article 58 de l'RGPD, tant els d'investigació com els correctius, com per exemple "imposar una limitació temporal o definitiva del tractament, inclosa la prohibició".

3. Descripció sistemàtica del tractament

Punts clau

- És essencial donar una descripció sistemàtica del tractament, per conèixer els riscos potencials que implica.
- Proposem una llista de preguntes que ajudaran el responsable de les dades a fer aquesta descripció; es remarquen els aspectes més rellevants des del punt de vista dels riscos.

Per poder determinar de forma acurada quins riscos poden afectar un tractament, cal conèixer amb detall el tractament i el context on es produeix. Proposem la següent llista de preguntes, com una guia que el responsable del tractament pot fer servir per descriure el tractament. L'objectiu de les preguntes és posar en relleu aspectes que poden ser clau a l'hora de determinar els riscos del tractament[3].

3.1 Quin és el tractament de dades?

L'objectiu d'aquesta pregunta és delimitar l'operació de tractament que s'està considerant, alhora que se'n fa una primera descripció.

Quines operacions de tractament es poden avaluar en una AIPD?

Una AIPD pot fer referència a una o a múltiples operacions de tractament, si són similars en termes de tipus de dades, abast, context, finalitat i riscos.

També és pot fer una AIPD per avaluar l'impacte que té una aplicació o plataforma de tractament. Això no eximeix el responsable del tractament que faci ús d'aquesta aplicació o plataforma de fer una AIPD adaptada al seu cas, però la pot basar en la de l'aplicació.

[3] *Guidelines for SME on the security of personal data processin*, ENISA, desembre 2016

Exemples

- Un hospital gestiona dades mèdiques de pacients: historial mèdic, dades de contacte, etc.
- El sistema de recursos humans d'una empresa gestiona dades personals del seu personal: dades de contacte, dades bancàries, retribucions, períodes de baixa i de vacances.

3.2 Quina és la finalitat del tractament?

Segons l'RGPD, la finalitat d'un tractament ha de ser explícita, legítima i determinada abans de recollir les dades.

L'obligació del responsable d'especificar la finalitat del tractament abans d'iniciar-lo ajuda les persones interessades a entendre l'ús que es farà de les seves dades; d'aquesta manera, permet que les persones interessades prenguin decisions informades respecte de l'ús de les seves dades. A banda, evita que, un cop recollides, les dades s'usin amb altres finalitats.

El principi de limitació de la finalitat està estretament relacionat amb altres principis, com ara el de licitud, lleialtat i transparència. La transparència exigeix que les persones interessades tinguin coneixement de l'ús que es fa de les seves dades. No es pot avaluar la licitud i la lleialtat d'un tractament si no se'n coneix la finalitat.

Exemples

- Una empresa tracta les dades dels seus clients amb la finalitat exclusiva de complir amb les seves obligacions comptables.
- El departament de màrqueting d'una empresa vol fer ús de les dades dels seus clients per enviar publicitat.

Tot i que en els casos anteriors les dades tractades poden ser les mateixes, la finalitat és molt diferent. Això fa que la base legal del tractament també sigui diferent. En el primer cas, el responsable de les dades fa el tractament per complir amb una obligació legal. En el segon cas, l'única base legal possible és el consentiment.

3.3 Tipus i característiques de les dades a tractar

Tot i que aquesta pregunta està relacionada amb l'operació de tractament (pregunta 1), convé especificar clarament quins són els tipus i les característiques de les dades a tractar. Això té importància a l'hora de determinar els riscos associats a l'operació de tractament, les seves bases legals i la manera d'obtenir consentiment.

Les característiques més rellevants de les dades són:

3.3.1 Font de les dades

Convé especificar si les dades s'han obtingut directament de la persona interessada o bé d'una tercera part i, si és així, especificar-la.

3.3.2 Termini de conservació

Les dades no s'han de conservar més temps del necessari per assolir la finalitat del tractament.

3.3.3 Dades especialment sensibles

L'RGPD parla de categories especials de dades personals per referir-se als tipus de dades que, per la seva naturalesa, presenten uns riscos més grans per als drets i les llibertats de les persones. L'RGPD limita el tractament que es pot fer d'aquestes dades. Els següents tipus de dades formen part de les categories especials de dades:

- Origen ètnic o racial
- Opinions polítiques
- Conviccions religioses o filosòfiques
- Afiliació sindical
- Dades genètiques
- Dades biomètriques capaces d'identificar de manera unívoca una persona
- Dades relatives a la salut
- Dades relatives a la vida o l'orientació sexual d'una persona

Tot i no estar contingudes dins les categories especials, el tractament de dades relacionades amb condemnes o infraccions penals també està subjecte a més restriccions.

De la mateixa manera, les dades de persones vulnerables (en particular, els menors) també reben una protecció especial.

3.3.4 Ús amb una finalitat diferent de la que va motivar la recollida

Si es volen utilitzar dades amb una finalitat diferent de la que va motivar-ne la recollida, cal aplicar certs controls per garantir que la nova finalitat és compatible.

3.4 Quins actors intervenen en el tractament?

A banda del actors essencials a què l'RGPD fa referència (el responsable i l'encarregat del tractament, les persones interessades i el DPD), el tractament es pot veure condicionat per altres actors. Convé determinar quins són i quins rols i responsabilitats tenen en el tractament.

3.5 Quins són els processos de tractament?

Les dades es poden tractar de forma automatitzada, de forma manual o amb una combinació de totes dues; ho pot fer el responsable del tractament o delegar-ho en un encarregat; es pot fer amb els mitjans propis del responsable del tractament o amb mitjans proporcionats per un encarregat (per exemple, al núvol).

Hi ha una estreta relació entre els mitjans que s'utilitzen per tractar les dades i els riscos del tractament. A banda, l'ús d'algunes tecnologies pot tenir implicacions que entren en conflicte amb altres aspectes de l'RGPD. Per exemple, l'ús d'un núvol podria implicar la transferència de dades fora de les fronteres de la UE, cosa que l'RGPD limita.

3.6 On es fa el tractament de les dades?

Seguint el criteri del GT29, no considerem que el tractament de dades fora de la UE sigui un factor a l'hora de determinar si cal fer una AIPD. Ara bé, això no vol dir que no sigui un factor important a l'hora d'executar l'AIPD.

La transferència de dades personals a un tercer país o organització internacional on l'RGPD no és d'aplicació pot fer que les persones interessades vegin reduïda la protecció de les seves dades. Per això l'RGPD restringeix aquestes transferències, que només es poden fer si es dona una de les condicions següents:

- La Comissió Europea considera que el tercer país, territori, sector d'un país o organització internacional ofereix un nivell de protecció adequat. El setembre de 2019 la llista de països reconeguts són: Andorra, Argentina, Canadà (organitzacions comercials), Estats Units (limitat al Privacy Shield), Guernsey, Illa de Man, Illes Faroe, Israel, Japó, Jersey, Nova Zelanda, Suïssa i Uruguai.

- Si el responsable o l'encarregat proporcionen les garanties adequades i les persones interessades disposen de drets exigibles i accions legals efectives. Les garanties adequades poden ser aportades per:

    - Un instrument jurídicament vinculant i exigible entre autoritats o organismes públics.
    - Normes corporatives vinculants, d'acord amb l'article 47 de l'RGPD.
    - Clàusules tipus de protecció de dades adoptades per la Comissió.
    - Clàusules tipus de protecció de dades adoptades per una autoritat de control i aprovades per la Comissió.
    - Un codi de conducta d'acord amb l'article 42 de l'RGPD, juntament amb compromisos vinculants i exigibles del responsable o de l'encarregat del tractament en el tercer país d'aplicar les garanties adequades.

- És d'aplicació alguna de les excepcions relacionades a l'article 49 de l'RGPD.

    - La persona interessada ha donat el consentiment a la transferència.
    - La transferència és necessària per executar un contracte entre la persona interessada i el responsable.
    - La transferència és necessària per executar un contracte, en interès de la persona interessada, entre el responsable del tractament i una tercera part.
    - La transferència és necessària per raons d'interès públic.
    - La transferència és necessària per formular, exercir o defensar reclamacions.
    - La transferència és necessària per protegir els interessos vitals de la persona interessada o d'altres persones, quan la persona interessada està incapacitada per donar el seu consentiment.
    - La transferència es fa des d'un registre públic que té per objecte facilitar informació al públic i que està obert a la consulta del públic en general.

4. Necessitat i proporcionalitat del tractament

Punts clau

- Cal que el tractament sigui eficaç per assolir la seva finalitat.
- Un tractament és necessari quan la finalitat no es pugui assolir de manera menys intrusiva.
- Un tractament és proporcionat quan els beneficis són superiors als perjudicis potencials.

En la descripció del tractament feta anteriorment, se n'ha fixat la finalitat. Ara cal avaluar la proporcionalitat i la necessitat del tractament, en relació amb aquesta finalitat.

Així doncs, cal avaluar si el tractament descrit a la secció anterior és idoni per assolir la finalitat, si hi ha una alternativa perquè sigui menys lesiu per als drets i les llibertats de les persones i si el benefici que s'obté del tractament és superior als potencials perjudicis que pot tenir sobre les persones.

En l'avaluació de la necessitat i la proporcionalitat, cal seguir la guia que estableixen els principis bàsics que han de regir qualsevol tractament de dades personals (art. 5 RGPD). En particular, hi tenen una incidència directa els principis de licitud, lleialtat, minimització de dades, limitació del termini de conservació de les dades i exactitud.

A banda d'avaluar els principis anteriors, per establir la necessitat i la proporcionalitat d'un tractament resulta indispensable identificar els riscos per als drets i les llibertats de les persones que implica el tractament, el nivell d'aquests riscos i, si escau, proposar mesures per mitigar-los. A la secció 6 s'analitzen els riscos des del punt de vista de la seguretat de la informació; és a dir, quins efectes pot tenir sobre les persones una pèrdua de la confidencialitat, de la integritat o de la disponibilitat de la informació. L'anàlisi que fem en aquesta secció pretén determinar l'impacte que té el tractament sobre les persones, si es produeix tal i com està planejat; és a dir, sense tenir en compte factors externs que el puguin alterar.

4.1 Avaluació de la finalitat del tractament

4.1.1 Tractament amb una finalitat diferent de la que va motivar la recollida

En general, les dades s'han de tractar exclusivament amb la finalitat per a la qual s'han recollit. Si es volen tractar dades amb una finalitat diferent, cal que la nova finalitat sigui compatible amb la inicial, llevat que es doni una de les condicions següents[4]:

- S'ha obtingut el consentiment de les persones interessades per al nou tractament.
- El tractament està basat en el dret de la Unió o dels estats membres que constitueixi una mesura per salvaguardar els objectius indicats en l'article 23:
    - Seguretat nacional.
    - Defensa.
    - Seguretat pública.

[4] Article 6.4 RGPD.

- Prevenció, investigació, detecció i processament de delictes penals.
- Altres objectius importants d'interès públic.
- La protecció de la independència judicial i dels procediments judicials.
- La prevenció, investigació, detecció i processament d'infraccions en normes deontològiques.
- La protecció de la persona interessada o dels drets i llibertats d'altres.
- L'execució de demandes civils.

4.1.2 Compatibilitat de finalitats

Per avaluar si una nova finalitat és compatible amb la finalitat que va motivar la recollida de dades, cal tenir en compte els aspectes següents:

- Les possibles relacions entre la nova finalitat i la finalitat inicial.
- El context en què s'han recollit les dades. En particular, si la persona interessada pot anticipar el nou tractament.
- La naturalesa de les dades. En particular, pel que fa a categories especials (art. 9 RGPD) i a dades de condemnes i delictes penals (art. 10 RGPD).
- Les possibles conseqüències del nou tractament.
- Si hi ha garanties adequades.

Com a norma general, si la nova finalitat és molt diferent de la inicial i no és una finalitat que les persones interessades puguin preveure, o pot tenir un impacte injustificat sobre les persones, s'ha de considerar incompatible amb la finalitat inicial.

El tractament de dades personals amb finalitat d'arxiu en l'interès públic, amb finalitat d'investigació científica o històrica o amb finalitat estadística es considera compatible amb la finalitat inicial[5].

4.2 Principi de licitud i lleialtat

4.2.1 Licitud

Perquè un tractament sigui lícit, cal que li sigui d'aplicació algun dels supòsits següents que donen una base legal al tractament:

[5] Article 6.4 RGPD.

- La persona interessada ha donat el seu consentiment per al tractament de les seves dades personals, per a una o diverses finalitats específiques.
- El tractament és necessari per executar un contracte en què la persona interessada n'és part o per aplicar mesures precontractuals.
- El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.
- El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física.
- El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.
- El tractament és necessari per satisfer els interessos legítims del responsable del tractament o d'un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de la persona interessada (en particular, quan és un menor).

A banda, cal que l'ús de les dades que facin el responsable i l'encarregat del tractament sigui lícit en un sentit ampli. Per exemple, l'ús que en facin no pot:

- Incórrer en cap il·lícit (civil o penal).
- Infringir la normativa del copyright.
- Infringir acords contractuals.

A l'hora d'escollir la base legal sobre la qual s'ha de fonamentar el tractament, cal tenir- ne en compte la finalitat i el context. S'ha de triar la base legal que encaixa millor amb les circumstàncies. No hi ha una base legal millor o més important que les altres. Pot ser, fins i tot, que el tractament es pugui acollir a més d'una base legal. En aquest cas, cal especificar totes les bases legals de bon començament.

Algunes de les bases legals tenen una finalitat específica: un contracte amb la persona interessada, una obligació legal, protegir els interessos vitals d'una persona i l'interès públic. Si el tractament es fa amb alguna d'aquestes finalitats, la base legal apropiada és òbvia.

Si el tractament es fa amb altres finalitats, llavors la base legal pot no ser tan òbvia. En molts casos hi pot haver l'opció de triar entre interessos legítims i consentiment. Si s'utilitza l'interès legítim com a base legal, es manté el control del tractament; però cal demostrar que està dins el que les persones poden raonablement esperar i que no els causa danys injustificats. Si s'utilitza el consentiment com a base legal, es dona a les persones interessades control total sobre l'ús de les seves dades (inclosa la possibilitat que retirin el consentiment i que no es pugui continuar tractant les seves dades).

Convé triar la base legal adequada des del principi. Si després d'iniciar el tractament es descobreix que la base legal era inadequada, pot ser difícil canviar-la per una altra. Fins i tot

si s'ha pogut aplicar des del principi, pot ser que les persones interessades no entenguin aquest canvi.

Exemple

Una organització decideix tractar dades personals sobre la base del consentiment. Després de recollir el consentiment de les persones interessades i iniciar el tractament, hi ha una persona que vol retirar el consentiment. L'organització, que vol seguir tractant les dades, decideix continuar el tractament sobre la base de l'interès legítim.

En aquest cas, s'ha fet creure a les persones interessades que controlaven el tractament de les seves dades, quan realment no era així. L'organització hauria hagut de deixar clar des del principi que el tractament es fonamentava en l'interès legítim i, en aquesta situació, hauria de deixar de tractar les dades quan es retira el consentiment.

4.2.1.1 Tractament de dades de menors

Els menors necessiten una protecció especial en el tractament de les seves dades, perquè poden no ser conscients dels riscos que comporta.

En particular, quan el tractament està relacionat amb l'oferta directa de serveis de la societat de la informació a nens i la base legal és el consentiment, l'RGPD estableix una edat mínima de 16 anys perquè el consentiment sigui vàlid. Si el menor té menys de 16 anys, cal que el consentiment el doni o l'autoritzi el titular de la pàtria potestat.

Els estats membres poden reduir l'edat mínima per donar consentiment, però no pot ser inferior a 13 anys. En el cas espanyol, l'edat s'ha fixat en 14 anys.

La taula següent mostra les edats mínimes per donar consentiment en el context de l'oferta directa de serveis de la societat de la informació:

Edat mínima de consentiment (a juliol de 2019)[6]

13 anys	14 anys	15 anys	16 anys
Bèlgica	Àustria	República Txeca	Alemanya
Dinamarca	Bulgària	França	Croàcia
Estònia	Espanya		Eslovàquia
Finlàndia	Itàlia		Eslovènia
Letònia	Lituània		Grècia
Malta	Xipre		Holanda
Portugal			Hongria
Regne Unit			Irlanda
Suècia			Luxemburg
			Polònia
			Romania

4.2.1.2 Tractament de categories especials de dades

Les dades de categories especials són més sensibles i necessiten més protecció. Quan es tracten aquestes dades, a banda de determinar una base legal per al tractament, cal determinar quina de les condicions de l'article 9 és la que permet tractar-les:

- La persona interessada ha donat el seu consentiment explícit per al tractament amb una finalitat específica, tret que el dret de la UE o de l'estat membre no ho permeti.
- El tractament és necessari per complir obligacions o per exercir drets en l'àmbit
- del dret laboral i de la seguretat i la protecció social.
- El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona, i la persona interessada no està capacitada per donar el consentiment.

[6] www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751

- El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física.
- El tractament és legítim i amb garanties, fet per una associació sense ànim de lucre de caràcter polític, filosòfic, religiós o sindical, sempre que el tractament afecti persones amb qui mantenen contactes en relació amb aquestes finalitat s i les dades no es comuniquin a tercers sense el consentiment de les persones interessades.
- El tractament fa referència a dades que la persona interessada ha fet públiques.
- El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.
- El tractament és necessari per raons d'interès públic essencial.
- El tractament és necessari per a finalitats de medecina preventiva o laboral, avaluació de la capacitat laboral del personal, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social.
- El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.
- El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.

La base legal triada per al tractament no restringeix les bases legals per al tractament de dades de categoria especial. Per exemple, l'ús del consentiment com a base legal no implica l'ús de consentiment explícit com a base per al tractament de dades de categories especials. Tot i això, hi ha casos en què l'enllaç entre un i l'altre és probable. Per exemple, si la base legal és l'interès vital, és probable que la base per al tractament de categories especials sigui la mateixa.

4.2.1.3 Tractament de dades penals

Tot i no ser una categoria especial de dades, les dades sobre condemnes o infraccions penals també gaudeixen d'una protecció especial. El tractament d'aquestes dades només està permès sota la supervisió de les autoritats públiques o quan ho autoritzi el dret de la unió o de l'estat membre. A més, s'estableix que els registres exhaustius de condemnes criminals només es poden mantenir sota control de l'autoritat.

4.2.1.4 Validesa del consentiment

Quan la base legal d'un tractament és el consentiment, perquè sigui vàlid cal que es compleixin les condicions següents:

- El responsable ha de poder demostrar que l'ha recollit.
- La sol·licitud de consentiment és intel·ligible, de fàcil accés i en un llenguatge clar.

- L'execució d'un contracte no es pot supeditar a rebre el consentiment respecte de dades personals no necessàries per executar el contracte.
- S'ha informat les persones interessades de la possibilitat de retirar el consentiment en qualsevol moment.

La retirada del consentiment no afecta la validesa dels tractaments fets abans de retirar-lo.

4.2.2 Lleialtat

Un tractament és lleial si fa un ús de les dades que sigui previsible per a les persones interessades (en relació amb la finalitat del tractament) i no se'n deriven conseqüències adverses per a les persones interessades que no siguin justificables.

4.3 Principi de minimització

El principi de minimització de dades determina que les dades han de ser adequades (suficients per acomplir amb la finalitat del tractament de forma adequada), rellevants (tenen relació amb la finalitat del tractament) i limitades a l'estrictament necessari per acomplir la finalitat del tractament. Aquest és un punt clau a l'hora de justificar la necessitat.

Per complir el principi de minimització, cal identificar quina és la mínima informació necessària per acomplir amb la finalitat d'un tractament. S'ha de recollir aquesta informació mínima i no més.

A banda del tipus de dades que es tracten, el nivell de detall d'aquestes dades també és essencial a l'hora de determinar si es compleix el principi de minimització. Les dades han de tenir un nivell de detall que sigui rellevant per a la finalitat del tractament.

Pot ser que les dades rellevants per al tractament variïn segons la persona o el grup de persones. En aquest cas, cal ajustar les dades recollides a les que són rellevants en cada cas.

Cal revisar de forma periòdica que les dades emmagatzemades continuen essent rellevants i adequades per a la finalitat del tractament, i esborrar qualsevol dada que no ho sigui.

Pel que fa a l'adequació de les dades, cal garantir que siguin útils per assolir la finalitat del tractament. No s'han de tractar dades insuficients o incompletes per a la finalitat pretesa.

4.4 Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament. Assegurar-se que s'esborren les dades personals quan deixen de ser necessàries redueix el risc que esdevinguin irrellevants, excessives o inexactes.

D'acord amb l'article 30.1, quan sigui possible cal establir i documentar uns períodes estàndard de retenció per als diferents tipus de dades. També convé assegurar-se que l'organització té els procediments necessaris per revisar i fer efectius aquests períodes de retenció.

El reglament no especifica quan de temps s'han de conservar les dades. És el responsable del tractament qui ha de fixar-ne el període de retenció, d'acord amb les necessitats del tractament. No s'han de conservar les dades de forma indefinida, en previsió que puguin ser necessàries en el futur.

Les dades es poden conservar indefinidament amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística. En aquests casos, cal garantir que s'implanten les mesures tècniques i organitzatives necessàries per garantir el principi de minimització. Tècniques com ara l'anonimització o la pseudonimització de les dades tenen una particular rellevància en aquest context.

4.5 Principi d'exactitud

El tractament de dades inexactes pot afectar negativament les persones. El principi d'exactitud demana que les dades siguin exactes i que es prenguin les mesures adequades per garantir que les que siguin inexactes s'actualitzin o s'esborrin sense dilació.

4.6 Riscos del tractament

Qualsevol tractament de dades pot tenir efectes negatius sobre els drets i les llibertats de les persones. Per pal·liar aquests efectes, l'RGPD proposa un enfocament basat en el risc. Les mesures per protegir els drets i les llibertats de les persones han de ser proporcionals al risc associat al tractament.

Típicament, l'avaluació del risc es fa des del punt de vista de l'organització que tracta les dades. És a dir, se centra en els efectes negatius sobre el responsable o l'encarregat del tractament. L'RGPD canvia aquest punt de vista i busca avaluar el risc del tractament sobre les persones.

La seguretat de la informació és el punt central en les avaluacions de risc. És a dir, normalment s'avaluen els potencials efectes negatius d'una violació de seguretat en el tractament. Ara bé, un tractament pot afectar els drets i les llibertats de les persones, encara que no s'hagi produït cap violació de la seguretat. Per exemple, un tractament pot ser discriminatori en si mateix o pot afavorir l'aparició de pràctiques discriminatòries. Aquesta secció se centra en aquesta darrera visió: l'avaluació del risc d'un tractament tal com ha estat dissenyat.

Comentari

Convé notar que qualsevol tractament de dades, siguin personals o no, pot tenir efectes negatius sobre les persones. A l'hora de fer una AIPD, només ens interessen els efectes derivats de l'ús de dades personals.

Per exemple, un tractament que es basa en dades agregades (per tant, no personals) pot tenir un efecte significatiu sobre un grup de persones.

Els efectes negatius que un tractament pot tenir sobre les persones depenen del tractament concret que s'està fent. Tot seguit en donem alguns exemples. Ara bé, és el responsable del tractament qui n'ha de determinar els efectes negatius potencials.

- Pèrdua de temps
- Enuig
- Augment dels costos
- Falta de comprensió
- Estrès
- Impossibilitat d'accedir a serveis o altres oportunitats
- Discriminació
- Robatori de la identitat i altres fraus
- Pèrdues econòmiques
- Danys psicològics
- Danys per a la reputació
- Danys físics
- Afectació de la salut
- Pèrdua de la feina
- Danys físics o psicològics greus

A l'hora de determinar els efectes que un tractament pot tenir sobre les persones, convé tenir en compte algunes característiques del tractament, com ara:

- El tipus de dades personals. El tractament de categories especials de dades, com ara l'origen racial o ètnic, les dades mèdiques o dades sobre les preferències polítiques, són clars indicadors de potencials efectes negatius sobre els drets i les llibertats de les persones. Ara bé, cal remarcar que altres tipus de dades que no formen part de les categories especials també poden tenir un impacte important. Per exemple, localitzacions, informació financera, etc.

- El grau de sensibilitat del tractament. Més enllà del tipus de dades tractades, el tipus de tractament també pot indicar potencials impactes. Per exemple, quan el tractament té com a objectiu la monitorització de persones.

- La quantitat de dades personals tractades sobre cada individu. Com més gran sigui aquesta quantitat, més gran seran els potencials efectes negatius sobre les persones.

- L'activitat del responsable del tractament. Per exemple, si l'activitat del responsable de tractament està relacionada amb la salut o les finances, ja podem entreveure que l'impacte pot ser alt.

- Les característiques de les persones interessades. Si les persones interessades formen part d'un grup amb necessitats especials (per exemple, menors o autoritats públiques), cal tenir una cura especial a l'hora de determinar els efectes potencials del tractament.

L'RGPD estableix la conveniència de tenir en compte l'opinió de les persones interessades a l'hora de fer una AIPD. Ja que l'avaluació del risc se centra en les persones (i no en l'organització que fa el tractament), aquest és un punt on resulta interessant recollir l'opinió de les persones interessades: els potencials efectes negatius, el nivell d'impacte, les amenaces i les probabilitats que aquestes amenaces es materialitzin.

4.6.1 Impacte

Un cop identificats els potencials efectes negatius, cal determinar quin impacte tenen. Considerem quatre nivells d'impacte: baix, mitjà, alt i molt alt.

Impacte	Descripció
Baix	Les persones interessades poden patir algunes molèsties menors, que poden superar sense problemes (per exemple, pèrdua de temps, enuig, etc.)
Mitjà	Les persones interessades poden trobar inconvenients importants, que poden superar amb algunes dificultats (per exemple, augment de costos, falta de comprensió, estrès, danys físics, impossibilitat d'accedir a algun servei, etc.)
Alt	Les persones interessades poden patir conseqüències importants, que poden superar amb dificultats importants (per exemple, discriminació, robatori de la identitat, pèrdues econòmiques, danys psicològics, danys per a la reputació, danys físics, empitjorament de la salut, pèrdua de la feina etc.)
Molt alt	Les persones interessades poden patir conseqüències greus que no poden superar (per exemple, danys físics o psicològics greus, mort, etc.)

Igual que abans, la responsabilitat de fer un càlcul acurat del nivell d'impacte recau sobre el responsable del tractament.

4.6.2 Amenaces i probabilitat

Tot i que un tractament pot tenir efectes negatius sobre una persona, aquests efectes no es materialitzen sempre. Per avaluar el risc associat un potencial efecte negatiu, cal estimar la probabilitat que es materialitzi.

Considerem tres nivells de probabilitat:

- Baixa. És improbable que l'impacte es materialitzi.
- Mitjana. És possible que l'impacte es materialitzi.
- Alta. És probable que l'impacte es materialitzi.

Aquesta probabilitat es podria estimar de forma directa. Ara bé, sense una anàlisi de les circumstàncies en què l'impacte és materialitza, l'estimació pot ser poc acurada. Per això, estimarem la probabilitat segons les amenaces.

Una amenaça és qualsevol circumstancia que té el potencial de materialitzar un dels efectes negatius descrits anteriorment. Un cop determinades les amenaces, cal calcular en quina mesura és probable. Tot i que aquesta estimació també és subjectiva, està més ben fonamentada.

4.6.3 Determinació del risc

El nivell de risc associat resulta de combinar la gravetat de l'impacte amb la probabilitat que es materialitzi. Atès que les darreres s'han calculat de manera qualitativa, l'estimació del risc també serà qualitativa.

A l'hora de calcular el nivell de risc és fonamental prendre el punt de vista de les persones interessades. Des del punt de vista del responsable o de l'encarregat del tractament, un impacte de molta gravetat podria ser acceptable, si la probabilitat és petita; el responsable podria decidir assumir el cost associat a aquest esdeveniment. Ara bé, el punt de vista de les persones afectades acostuma a ser diferent, ja que l'impacte recau sobre elles. Això fa que, en general, no vulguin impactes amb gravetat molt alta encara que la probabilitat sigui baixa, ja que refer-se d'aquests impactes podria ser molt difícil, o fins i tot impossible. A més, tot i que hi pugui haver persones disposades a acceptar un impacte de gravetat molt alta, si la probabilitat és baixa no és apropiat que el responsable del tractament prengui aquesta decisió.

Proposem la taula de càlcul de risc següent. D'acord amb el que s'ha exposat, si el potencial impacte és molt alt, el risc serà alt independentment de la probabilitat.

	Impacte			
Probabilitat	Baix	Mitjà	Alt	Molt alt
Alta	Risc mitjà	Risc alt	Risc alt	Risc alt
Mitjana	Risc baix	Risc mitjà	Risc alt	Risc alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc alt

4.6.4 Reducció dels riscos

Llevat que el risc sigui baix, cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt o molt alt. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar l'autoritat de protecció de dades competent sobre la idoneïtat del tractament.

Les mesures que es poden prendre depenen del tractament i és tasca del responsable del tractament trobar les més adients. Algunes mesures poden ser:

- Evitar la recollida de certs tipus de dades.
- Reduir l'abast del tractament.
- Formar el personal perquè faci un ús apropiat de la informació.
- Anonimitzar o pseudonimitzar les dades.
- Tenir una política clara de compartició de dades.

En el cas del risc associat a la seguretat de la informació, és habitual calcular un risc inicial (sense controls de seguretat) i un risc residual (amb els controls implementats per reduir el risc inicial). Això és possible perquè els controls de seguretat no alteren l'essència del tractament. Ara bé, en el cas del risc associat al tractament tal com està dissenyat, les mesures per reduir-lo són, bàsicament, modificacions del disseny del tractament. Modificar-ne el disseny de forma separada a la descripció del tractament feta a la secció anterior faria que la descripció inicial no fos acurada. Això no és convenient i, per tant, cal adaptar les seccions anteriors de l'AIPD als canvis fets al tractament i tornar a calcular el risc. Això fa que fer una AIPD no sigui un tasca lineal.

Exemple

Una empresa posa en marxa un procés de selecció per contractar personal. L'objectiu d'aquest procés de selecció és triar la persona més adequada per fer una feina.

En un sentit ampli de la paraula, qualsevol procés de selecció discrimina. Ara bé, volem que aquesta discriminació estigui justificada per la capacitació de les persones i no per motius espuris.

Pot ser que per motius de comunicació amb els candidats es reculli informació del lloc de residència. Un avaluador amb accés a aquesta informació pot deixar fora (discriminar) els candidats que visquin en zones marginals. Si qualifiquem l'impacte d'aquesta potencial discriminació d'alt i li assignem una probabilitat mitjana, en resulta un risc alt. Cal buscar mesures per reduir-lo.

Convé notar que conèixer el domicili de residència no és necessari per avaluar la capacitació del candidats. Per tant, una mesura per reduir el risc seria privar els avaluadors d'aquesta informació.

4.7 Necessitat i proporcionalitat del tractament

Un cop avaluats els principis de protecció de dades i analitzats quins són els riscos per als drets i les llibertats de les persones, el responsable té la informació necessària per avaluar la necessitat i la proporcionalitat del tractament.

Un tractament només té sentit si assoleix la seva finalitat. Per tant, justificar l'eficàcia del tractament és un primer pas essencial per justificar-ne la necessitat.

Per justificar que un tractament és necessari, cal mostrar que no hi ha cap altre tractament que sigui, alhora, efectiu i menys lesiu per als drets i les llibertats de les persones.

Per justificar que un tractament és proporcional, cal mostrar que el benefici que s'obté del tractament és superior als perjudicis potencials sobre les persones. En la justificació de la proporcionalitat, convé tenir en compte l'anàlisi de risc fet a la secció anterior.

4.8 Opinió de les persones interessades

El responsable del tractament ha de buscar l'opinió de les persones interessades sobre l'operació de tractament. La necessitat i la proporcionalitat del tractament és un punt especialment interessant per buscar l'opinió de les persones interessades. Si no es considera apropiat buscar-la, cal documentar el perquè. Per exemple, per què té un cost desproporcionat o per què pot posar en risc la confidencialitat del pla de negoci.

5. Protecció dels drets de les persones

Punts clau

- El Reglament estableix una sèrie de drets que permeten a les persones conèixer i intervenir en el tractament de les seves dades.
- A l'hora d'avaluar l'impacte del tractament, és essencial garantir que les persones poden exercir aquests drets.

Els principis fonamentals a què fa referència l'article 5 del Reglament es materialitzen en una sèrie de drets que s'estableixen al capítol 3: transparència, informació i accés a les dades personals, rectificació i supressió, limitació i oposició.

Aquests drets donen a les persones interessades la possibilitat de conèixer el tractament i d'intervenir-hi. La transparència i el dret a la informació són necessaris perquè les persones interessades siguin conscients de com es tracten les seves dades. Els drets d'accés,

rectificació i supressió permeten que les persones interessades controlin les seves dades. Els drets de limitació i oposició donen a les persones interessades control sobre el tractament.

És essencial garantir que les persones poden exercir els drets que tenen reconeguts al Reglament. L'objectiu d'aquesta secció és avaluar els mecanismes establerts per garantir-ho.

5.1 Transparència

El Reglament parla de la transparència com una propietat transversal, que ha de ser present a l'hora d'informar les persones interessades.

Més concretament, la transparència exigeix que qualsevol comunicació amb les persones interessades sigui concisa, intel·ligible i de fàcil accés, i que utilitzi un llenguatge clar i senzill. Especialment, quan aquesta comunicació estigui adreçada a un infant.

També exigeix que les sol·licituds de les persones interessades es tramitin en un temps raonable. En particular, el reglament estableix un període d'un mes, que es pot ampliar (prèvia notificació dins el termini d'un mes) en dos mesos addicionals, si ho justifica la complexitat o el nombre de sol·licituds.

Finalment, la transparència exigeix que, si no es tramita la sol·licitud d'una persona interessada, el responsable informi sense dilació d'aquest fet i de les raons, així com de la possibilitat de presentar una reclamació a una autoritat de control i d'exercir accions judicials.

En el curs d'una sol·licitud d'una persona interessada, i en el cas que el responsable tingui dubtes respecte de la identitat de la persona sol·licitant, la persona representant pot demanar la informació necessària per confirmar la identitat.

5.2 Dret d'informació

El dret d'informació estableix que les persones interessades tenen el dret d'estar informades de la recollida i posterior tractament que es fa de les seves dades. Aquest és un dret essencial perquè, sense aquesta informació, la resta de drets no es poden fer efectius.

El dret d'informació estableix que el responsable ha de donar la informació següent a les persones interessades:

- La identitat i les dades de contacte del responsable.
- Les dades de contacte del delegat de protecció de dades (si n'hi ha).
- La finalitat del tractament.
- La base legal del tractament.
- L'interès legítim del responsable, si aquesta és la base legal del tractament.
- Les persones destinatàries o categories de destinataris de les dades.
- El termini de conservació de les dades o el criteri emprat per determinar-lo.
- La intenció de transmetre les dades fora de la UE, si escau.
- La decisió de la Comissió Europea respecte de la suficiència de la seguretat que ofereix el país o organització destinatària.

A banda, per garantir que les persones interessades coneixen els seus drets i saben com exercir- los, cal que el responsable del tractament els informi que tenen els drets següents:

- Dret d'accés a les dades.
- Dret de rectificació i supressió.
- Dret de limitació del tractament.
- Dret d'oposició al tractament.
- Dret a la portabilitat de les dades.
- Dret a revocar el consentiment (si aquesta és la base legal del tractament).
- Dret a presentar una reclamació davant una autoritat de control.

I, així mateix:

- Que la comunicació de les dades és un requisit legal o contractual, si escau.
- L'existència de decisions automatitzades.

En el cas de dades que no s'han recollit directament de la persona interessada, cal informar de la seva procedència.

Quan les dades es recullen directament de les persones interessades, cal donar la informació la p anterior en el mateix moment de recollida. Quan les dades no es recullen directament de les persones interessades, cal informar:

- En un període raonable de temps i superior a un mes.
- Si ens comuniquem amb les persones interessades, com a molt tard en el moment de la primera comunicació.
- Si es volen comunicar les dades a tercers, abans de comunicar-les.

Hi ha algunes exempcions a l'obligació d'informar, que depenen de com s'han recollit les dades:

- Si les dades s'han obtingut directament de la persona interessada, no hi ha l'obligació d'informar-la si ja disposa de la informació.
- Si les dades no s'han obtingut directament de la persona interessada, no cal informar-la si es dona alguna de les següents condicions[7]: la persona interessada ja disposa d'aquesta informació, la comunicació és impossible o suposa un esforç desproporcionat, així està regulat per una norma de la UE o dels estats membres o la informació té caràcter confidencial sobre la base del secret professional.

Ara bé, en cas que no s'informi, cal justificar-ho.

5.3 Dret d'accés

La persona interessada té el dret d'obtenir del responsable del tractament la confirmació que s'estan tractant les seves dades i, en aquest cas, el dret d'accés a les dades personals i a la informació següent:

- La finalitat del tractament.
- Les categories de dades tractades.
- Les persones destinatàries de les dades.
- El termini de conservació de les dades.
- Els drets a rectificar i suprimir les dades.
- Els drets a limitar i oposar-se al tractament.
- El dret a reclamar davant una autoritat de control.
- Si les dades no s'han obtingut de la persona interessada, l'origen de les dades.
- L'existència de decisions automatitzades, si escau.
- Garanties en la transferència de dades fora de la UE, si escau.

A banda de conèixer quina informació s'ha de transmetre a les persones interessades, cal assegurar- se que es donen les condicions per fer efectiu el dret d'accés.

Com es reconeix una sol·licitud vàlida?

El Reglament no diu com s'han de fer les sol·licituds d'accés. És a dir, es poden adreçar a qualsevol treballador o treballadora, per qualsevol mitjà i no necessiten cap frase del tipus "sol·licitud del dret d'accés". Per aquesta raó, cal assegurar-se que el personal que interacciona amb les persones interessades té els coneixements suficients per identificar les sol·licituds.

[7] RGPD, article 14.5.

Cal establir un procediment per fer les sol·licituds?

És recomanable establir un procediment estàndard per fer les sol·licituds. Això facilita les coses tant al responsable com a les persones interessades. Ara bé, les sol·licituds són igualment vàlides encara que no utilitzin aquest procediment.

La transparència és d'aplicació als procediments dissenyats per garantir el dret d'accés.

- La informació ha de ser concisa, intel·ligible, fàcilment accessible i en un llenguatge clar i senzill.
- Les sol·licituds s'han de tramitar en un termini d'un mes.
- Si la complexitat o el nombre de sol·licituds ho requereix, aquest termini es pot ampliar en dos mesos. Ara bé, cal informar-ne les persones interessades abans que finalitzi el primer mes.
- Si hi ha dubte sobre la identitat de la persona que fa la sol·licitud, es pot demanar la informació necessària per confirmar-ne la identitat.
- La sol·licitud ha de ser gratuïta. El responsable únicament les pot cobrar (o desestimar) si són infundades o excessives.

5.4 Dret de rectificació

El Reglament estableix el dret de les persones que es rectifiqui la informació personal que no sigui exacta. Ara bé, a l'hora de determinar si una informació és exacta també hi pot intervenir la percepció personal. Això fa que l'exercici d'aquest dret pugui tenir una certa complexitat.

Si es rep una sol·licitud de rectificació, cal fer els passos necessaris per comprovar si la informació és acurada i, si escau, rectificar-la.

Mentre s'està comprovant si les dades són exactes, la persona interessada pot demanar que es limiti el tractament[8].

Per la transparència, si el resultat de la comprovació és que la informació ja és exacta i, per tant, no cal rectificar-la, se n'ha d'informar la persona interessada. Cal explicar-li la decisió i informar-la de la possibilitat de recórrer a l'autoritat de protecció de dades competent.

[8] RGPD, article 18.

Segons l'article 19, si el responsable ha compartit les dades, ha de prendre les mesures adequades (tenint en compte els costos i la tecnologia disponible) per informar les persones destinatàries sobre la petició de rectificació.

5.5 Dret de supressió

Segons el Reglament, les persones tenen el dret que se n'esborri la informació quan es dona algun dels casos següents:

- Les dades ja no són necessàries en relació amb la finalitat per què es van recollir.
- La persona interessada retira el seu consentiment i no hi ha cap altra base legal per al tractament.
- La persona interessada s'oposa al tractament i no hi ha cap altre factor superior que la legitimi.
- Les dades s'han tractat sense una base legal.
- Les dades s'han d'esborrar d'acord amb una obligació legal que afecta el responsable.
- Les dades s'utilitzen per oferir serveis de la societat de la informació a infants.

Si el responsable ha compartit les dades, cal que prengui les mesures adequades (tenint en compte els costos i la tecnologia disponible) per informar les persones destinatàries sobre la petició.

El dret de supressió no és d'aplicació en els casos següents:

- Per exercir el dret a la llibertat d'expressió i d'informació.
- Per complir una obligació legal o en l'interès públic.
- Amb la finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, i amb finalitat estadística (si el compliment d'aquestes finalitats es veiés afectat per la supressió de les dades).
- Per presentar, exercir o defensar reclamacions legals.

5.6 Dret a limitar el tractament

L'article 18 dona a les persones el dret a limitar el tractament de les seves dades, en els casos següents:

- La persona interessada ha demanat la rectificació de les seves dades i el responsable està verificant si són exactes.
- Les dades s'han tractat sense una base legal.

- La persona interessada necessita que el responsable guardi les dades per iniciar, exercir o defensar una reclamació.
- La persona interessada s'ha oposat al tractament i el responsable està avaluant si els motius legítims del responsable prevalen sobre els de La persona interessada.

La noció de tractament és molt general: inclou, entre altres, recollida, anàlisi, disseminació i supressió de dades. És important que es tinguin en compte totes les formes de tractament, a l'hora de limitar-lo.

Si el responsable ha compartit les dades, cal que prengui les mesures adequades (tenint en compte els costos i la tecnologia disponible) per informar les persones destinatàries sobre la petició.

5.7 Dret a la portabilitat de dades

Segons l'article 20, les persones tenen el dret a demanar les dades que han facilitat al responsable del tractament en els següents casos:

- Si el tractament està basat en el consentiment, o és necessari per executar un contracte o per aplicar mesures precontractuals.
- El tractament es fa amb mitjans automatitzats.

El dret a la portabilitat de dades no es limita a les dades que les persones han donat de forma explicita; també afecta les dades que s'han recollit de l'observació de les persones. Per exemple, el registre de cerques que una persona ha fet en un buscador o la informació de localització recollida d'un GPS.

Les dades s'han de transmetre en un format estructurat d'ús comú i que sigui de fàcil lectura mecànica.

El dret a la portabilitat de dades no ha d'afectar negativament a altres persones. En particular:

- Si les dades personals contenen informació d'una tercera persona, cal avaluar si aquesta darrera pot veure afectats els seus drets i llibertats.
- Si les dades estan associades a diverses persones (per exemple, un compte bancari compartit), cal buscar el consens de totes les persones interessades.

5.8 Dret d'oposició

Segons l'article 21, les persones tenen el dret a oposar-se al tractament de la seva informació quan aquest tractament es fa sobre la base de:

- L'interès públic o l'exercici de poders públics conferits al responsable del tractament.
- L'interès legítim del responsable del tractament.

En aquest cas, el responsable ha de cessar en el tractament, llevat que acrediti motius legítims que prevalguin sobre els drets de la persona interessada.

El Reglament parla de les tres situacions següents:

- Oposició al tractament amb finalitats de màrqueting. En aquest cas, el responsable ha d'aturar el tractament sense excepció.
- Oposició al tractament amb finalitat d'investigació científica o històrica, o amb finalitat estadística. En aquest cas, el responsable pot continuar el tractament si està justificat per l'interès públic.

5.9 Dret a no ser objecte de decisions automatitzades

Segons l'article 22, les persones tenen el dret a no ser objecte de decisions basades únicament en el tractament automatitzat (inclosa l'elaboració de perfils), si tenen efectes jurídics o tenen un efecte significatiu, llevat que:

- Sigui necessari per executar un contracte entre la persona interessada i el responsable.
- Estigui autoritzat pel dret de la Unió o d'un estat membre.
- La persona interessada hagi donat el seu consentiment explícit.

La persona interessada sempre tindrà dret a obtenir intervenció humana, a expressar el seu punt de vista i a impugnar la decisió.

Aquestes decisions automatitzades només poden fer ús de categories especials de dades si hi ha el consentiment explícit de la persona interessada, o si el tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.

6. Riscos en la seguretat de les dades

D'acord amb l'RGPD, les mesures emprades per protegir la informació han de ser apropiades al risc per als drets i les llibertats de les persones. A la secció 4.6 s'han avaluat

els riscos associats al tractament, tal com està dissenyat. En aquesta secció, es busca avaluar els riscos des del punt de vista de la seguretat de la informació; és a dir, els riscos que presenta el tractament quan no es fa segons el disseny inicial.

Seguim el procés descrit a la secció 4.6: partint de la descripció del tractament feta amb anterioritat, avaluarem quin és l'impacte potencial sobre les persones i quina és la probabilitat que aquest impacte es materialitzi. Això ens permetrà calcular el risc inicial. Si el risc és massa gran, cal aplicar controls (mesures de protecció) per reduir-lo. Aquestes mesures poden buscar reduir la gravetat d'un impacte o la probabilitat que es materialitzi.

L'RGPD busca una solució que sigui el més completa possible. En particular, cita les següents mesures de protecció que cal considerar (entre d'altres)[9]:

- Pseudonimització i encriptació de les dades.
- Mesures per garantir la confidencialitat, integritat, disponibilitat i la resiliència dels sistemes de tractament i els serveis.
- En cas d'incident, mesures per recuperar la disponibilitat i l'accés a les dades personals en un temps adequat.
- Un procés continu de prova i avaluació de l'efectivitat de les mesures proposades per garantir la seguretat del tractament.

Els tres primers punts fan referència a mesures de protecció. Les mesures del primer punt busquen reduir la probabilitat que l'impacte es materialitzi, mentre que les mesures del tercer punt busquen reduir la severitat de l'impacte. El segon punt és més general i engloba tot tipus de mesures. L'últim punt fa referència al fet que el procés de gestió de risc no és un procés puntual, sinó que s'ha de fer un seguiment dels riscos i de l'efectivitat dels controls.

Pel que fa a la metodologia d'anàlisi de riscos, n'hi ha que tenen un ampli reconeixement, com ara: ISO 27005:2013, OCTAVE, NIST SP 800-30 i Magerit. Ara bé, fer una anàlisi de riscos emprant aquestes metodologies pot ser un procés complex. Per exemple, a Magerit hem de:

1. Identificar els actius del sistema (que poden ser informació, serveis, programari, maquinari, comunicacions, instal·lacions, etc.), especificar la relació de dependència que hi ha entre ells i avaluar-los.
2. Identificar les amenaces rellevants per al nostre sistema i caracteritzar-les segons la probabilitat que es materialitzin i la degradació que causen.

[9] RGPD, article 32.1.

3. Identificar els controls que cal desplegar al sistema i qualificar-ne l'eficàcia enfront de les amenaces identificades prèviament.

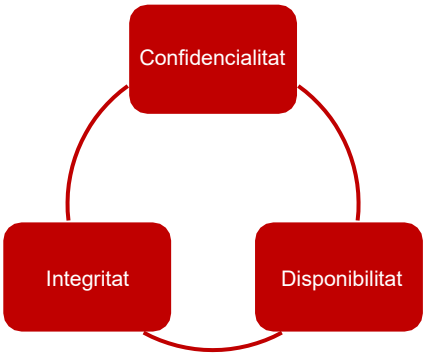
Amb l'objectiu de fer l'avaluació de riscos més assequible, aquesta guia proposa un mètode simplificat[10]. Si una organització té la capacitat suficient per abordar alguna de les metodologies d'anàlisi de riscos mencionades anteriorment, convé que ho faci però sense perdre de vista que l'objectiu és avaluar el risc sobre les persones (no sobre l'organització).

6.1 Breu introducció a la seguretat de la informació

Entenem per seguretat de la informació el conjunt de mesures (tècniques, organitzatives, etc.) que es prenen per protegir la informació que es tracta en un sistema contra l'accés no autoritzat, la revelació, la modificació i la destrucció.

El triangle CIA és un model de seguretat de la informació molt conegut. Fa referència a tres propietats essencials en la seguretat de la informació: confidencialitat, integritat i disponibilitat (*availability*, en anglès).

- Confidencialitat. Només poden accedir a la informació les persones, entitats o processos que han estat prèviament autoritzats.
- Integritat. Només poden modificar la informació les persones, entitats o processos que han estat prèviament autoritzats.
- Disponibilitat. La informació ha d'estar disponible quan una persona, entitat o procés autoritzat la demani.



Les tres propietats anteriors són bàsiques. Ara bé, hi ha models que les complementen amb altres propietats derivades. Per exemple, a l'ENS es parla també d'autenticitat i traçabilitat. En la nostra estimació de risc ens limitarem a les tres propietats bàsiques.

[10] Basat en la guia "*Guidelines for SMEs on the security of personal data processing*", ENISA.

6.2 Impacte

El primer pas per avaluar el risc és determinar la gravetat dels efectes sobre els drets i les llibertats de les persones que pot causar la pèrdua de la confidencialitat, de la integritat o de la disponibilitat de les dades. Cal remarcar que mentre que normalment es mesura l'impacte sobre l'organització, aquí mesurem l'impacte sobre les persones.

A l'hora d'avaluar l'impacte, s'han de considerar tots els possibles casos de pèrdua de la confidencialitat, de la integritat i de la disponibilitat. Per facilitar aquesta tasca, es plantegen diferents escenaris en què es perd alguna d'aquestes propietats.

Escenaris en què hi ha pèrdua de confidencialitat:

- Pèrdua o robatori d'un ordinador que conté dades personals.
- Enviament per error de dades personals a persones no autoritzades.
- Possibilitat d'accedir de forma no autoritzada al compte d'una persona.
- Un error de configuració en una web exposa les dades personals de les persones usuàries.
- Robatori d'informació de les instal·lacions del responsable o de l'encarregat del tractament.
- Un empleat d'un centre mèdic consulta de forma no autoritzada l'expedient d'un pacient.

Escenaris en què hi ha pèrdua de la integritat:

- Un empleat o empleada modifica per error les dades d'un client o clienta.
- Un error en la xarxa de comunicacions altera les dades mentre estan en trànsit.
- Per motius operacionals, una empresa manté diverses còpies de les dades, però un canvi en alguna de les còpies no és propaga a les altres.
- Pèrdua de part d'un expedient, com a conseqüència d'una fallada en el sistema de tractament.

Escenaris en què hi ha pèrdua de la disponibilitat:

- Un fitxer és corromp o s'esborra i no hi ha una còpia de seguretat.
- Es perd un expedient del qual només hi havia una còpia en paper.
- Un servei de consulta de dades deixa d'estar disponible (per exemple, el servei per accedir al registres electrònics de salut).

D'acord amb la secció 6.2, l'impacte sobre les persones de la pèrdua de la seguretat de les dades pot ser baix, mitjà, alt o molt alt. Per fixar el valor, cal tenir en compte les característiques del tractament. Les situacions següents incrementen el risc:

- El tractament dades de categories especials o altres dades especialment sensibles (informació financera, localitzacions, etc.).
- La monitorització de persones.
- El tractament de dades de grups amb necessitats especials (menors, autoritats, etc.).
- El tractament de gran quantitat de dades de cada persona.

Com a resultat, tindrem un impacte per la pèrdua de la confidencialitat, un per la pèrdua de la integritat i un per la pèrdua de la disponibilitat. També podem calcular l'impacte global del sistema de tractament, com el màxim dels impactes anteriors.

6.3 Probabilitat inicial

El risc es calcula d'acord amb l'impacte que té la pèrdua de les propietats de seguretat (confidencialitat, integritat i disponibilitat) i de la probabilitat que aquest impacte es materialitzi. L'objectiu d'aquesta secció és estimar aquesta probabilitat.

Amb l'objectiu de mantenir l'anàlisi simple, l'estimació de la probabilitat no es basarà en un inventari del sistema. Això requeriria identificar els actius, les amenaces i les vulnerabilitats. La nostra estimació es basa en la identificació d'algunes característiques del sistema de tractament que el fan més susceptible de patir atacs.

Considerem característiques del sistema de tractament dels tipus: maquinari i programari, processos de tractament, persones que intervenen en el tractament i altres característiques.

Maquinari i programari

El sistema de tractament està connectat a sistemes externs a l'organització?

La connexió amb sistemes externs a l'organització incrementa l'exposició a amenaces. Per exemple, la informació pot ser capturada o modificada maliciosament mentre està en trànsit.

Exemples

- El sistema de tractament d'un hospital està connectat amb els sistema públic de seguretat social i amb els sistemes de d'asseguradores privades.
- Les estacions de treball que formen part del sistema de tractament tenen accés a internet.

Alguna part del tractament es fa a través d'internet?

La interacció amb les persones interessades a través d'internet exposa el sistema de tractament a amenaces externes, com ara phishing, SQL injection, man-in-the-middle attacks, DoS i XSS. Aquestes amenaces poden comprometre el sistema de tractament i afectar les propietats de seguretat de les dades (confidencialitat, integritat i disponibilitat).

Permetre que el personal accedeixi al sistema de tractament a través d'internet també incrementa l'exposició a atacs externs i, a banda, incrementa la possibilitat que el personal faci un mal ús de la informació (accidental o intencionat).

Exemples

- Botiga en línia, banca en línia, etc.
- S'utilitza el correu electrònic en el tractament.
- Els administradors del sistema de tractament poden fer tasques de manteniment o supervisió a través d'internet.
- L'accés al sistema de tractament des d'un espai públic pot facilitar que persones alienes a l'organització puguin observar-les.

Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?

Si el sistema de tractament no està ben dissenyat o els elements que el componen no estan configurats adequadament, els riscos per a la seguretat de les dades s'incrementen. Hi ha multitud de guies de bones pràctiques en seguretat amb diferent temàtica (xarxa, equips, etc.).

Exemples

- Cal dissenyar la xarxa seguint un document de bones pràctiques que inclogui elements com ara tallafocs, segmentació de la xarxa i ús de VPN.
- Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el sistema operatiu. Això implica mesures com ara l'ús d'antivirus i no permetre l'ús de paraules de pas insegures.
- Cal dimensionar el sistema de tractament pensant en les necessitats computacionals, de comunicació i d'emmagatzematge que s'anticipen. També cal dotar-lo del personal suficient.

- Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el programari. Per exemple, com configurar un servidor web per fer-lo més segur.
- Cal usar una metodologia de desenvolupament que tingui en compte la seguretat de les dades durant tot el cicle de vida de l'aplicació.

Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?

És essencial fer un manteniment i una monitorització adequada del sistema. El manteniment s'ha de fer tant dels dispositius com del programari. Monitoritzar el sistema no només permet analitzar un incident un cop s'ha produït, sinó que també ajuda a detectar comportaments sospitosos a fi d'evitar que l'incident tingui lloc, o per reduir-ne l'impacte.

Exemples:

- No aplicar les actualitzacions de seguretat del sistema operatiu pot donar lloc a nous vectors d'atac.
- La manca de còpies de seguretat regulars pot donar lloc a la pèrdua d'informació en cas d'incident.

Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?

La seguretat física de les instal·lacions de tractament és essencial. Sense això, no es pot garantir la seguretat del sistema de tractament (ja sigui electrònic o no).

Exemples

- El CPD no està degudament protegit amb un sistema que impedeix l'accés a les persones no autoritzades.
- Les limitacions d'espai han fet que part de l'arxiu en paper s'hagi distribuït en diferents àrees, que no en garanteixen la seguretat.
- El CPD no està protegit contra accidents naturals i industrials (per exemple, fallades elèctriques, inundacions).
- És fa ús d'un servei al núvol sense tenir garanties que les instal·lacions proveïdor estan prou protegides.

Ús del sistema de tractament

Hi ha una manca de claredat en la definició dels rols i les responsabilitats del personal?

Una manca de claredat en la definició dels rols i les responsabilitats pot donar lloc a un ús descontrolat de les dades (ja sigui accidental o intencionat).

Exemples

- Un treballador o treballadora d'una oficina bancària només hauria de consultar les dades dels seus clients.
- El personal és responsable de destruir la informació (digital o no) de forma segura, quan deixa de ser necessària.
- El personal és responsable de mantenir la seguretat de les dades, quan les comunica a alguna altra persona o organització.

Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?

Quan els usos acceptables dels sistemes de tractament no estan definits clarament, s'incrementa el risc de fer-ne un mal ús i d'introduir vulnerabilitats al sistema.

Exemples

- La instal·lació de programari de compartició de fitxers pot donar lloc a la compartició involuntària de fitxers.
- La instal·lació de programari per part de persones usuàries no administradores pot donar lloc a un manteniment deficient.
- Visitar pàgines web malicioses pot ser una font d'entrada de programari maliciós i de robatori de dades.

Pot el personal connectar dispositius externs al sistema?

La connexió de dispositius externs al sistema de tractament és una porta a l'entrada de programari maliciós, d'introducció de vulnerabilitats, etc. A banda, també facilita l'extracció d'informació.

Exemples:

- El personal connecta el seu telèfon o el seu llapis de memòria als ports USB de l'ordinador.
- El personal pot emprar els seus dispositius per efectuar tasques relacionades amb el tractament (BYOD).

Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?

La manca d'un registre de les activitats (log file) pot incrementar les males pràctiques del personal i, alhora, dificulta la investigació dels incidents un cop s'han produït.

Exemples

- Es poden consultar els expedients de clients/pacients sense que en quedi un registre.
- Tot i que es genera un registre d'activitats, no es monitoritza.
- No hi ha constància de les persones que entren al CPD.

Persones

El personal rep permisos que no són necessaris per complir les tasques que té encomanades?

Com més gran sigui la base de persones que tenen accés a unes dades, més gran és la probabilitat que es produeixi un abús. Per evitar això, és essencial que el sistema controli l'accés al sistema del personal i autoritzi només els accessos que són estrictament necessaris per complir les tasques que té encomanades.

Exemples

- L'accés a l'historial clínic d'un pacient hauria d'estar limitat als equips professionals que el tracten.

S'ha externalitat alguna part del tractament a un encarregat?

L'externalització del tractament o part del tractament a un encarregat suposa una pèrdua de control sobre les dades. Cal escollir un encarregat que pugui oferir un nivell alt de seguretat i definir clarament les seves responsabilitats.

Exemples

- S'utilitza un núvol per realitzar part del tractament.
- Es contracten uns serveis especialitzats per analitzar unes dades.

Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD?

Una manca de coneixements sobre l'ús que s'espera del sistema, sobre seguretat de la informació o sobre les obligacions i limitacions que imposa l'RGPD pot donar lloc a males pràctiques.

Exemples

- La manca de coneixements en seguretat pot fer que el personal que tracta les dades sigui més propens a seguir les instruccions d'un correu de phishing.
- El personal ha de recordar la necessitat de desar els document físics sota les condicions de seguretat adequades.

Altres característiques

Ha patit l'empresa o altres empreses del sector atacs darrerament?

L'existència d'atacs anteriors s'ha de prendre com una advertència de potencials atacs futurs. Convé prendre les mesures necessàries per evitar que atacs similars tinguin èxit.

S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?

La presència d'errors en el sistema de tractament incrementa la probabilitat de patir un atac. De la mateixa manera, les advertències respecte de potencials fallades en la seguretat del sistema també poden indicar una probabilitat més alta de patir atacs.

Exemples:

- En entrar dades incorrectes en un formulari, l'aplicació de tractament mostra un error i finalitza de forma inesperada.
- S'ha rebut la notificació d'una persona usuària que el sistema és vulnerable a algun atac específic.

Es tracten dades d'especial interès o dades d'un nombre molt gran de persones usuàries?

La presència massiva de dades i la presència de dades d'especial interès són una motivació extra per a possibles atacants.

Exemple

- Una gran empresa que emmagatzema dades personals i financeres dels seus clients (per exemple, número de targeta de crèdit).

Cada resposta afirmativa en algun dels apartats de les taules anteriors indica un increment de la probabilitat que es materialitzi un impacte sobre la seguretat de les dades. Per estimar la probabilitat inicial (sense controls de seguretat), comptem el nombre de respostes afirmatives i apliquem la taula següent:

Respostes afirmatives	Probabilitat inicial
0 - 4	Baixa
5 – 9	Mitjana
10 - 15	Alta

6.4 Risc inicial

Un cop estimat l'impacte i la probabilitat inicial, ja podem donar l'estimació del risc inicial (sense els controls de seguretat). Seguim la mateixa taula que hem fet servir a la secció 4.6.

	Impacte			
Probabilitat	Baix	Mitjà	Alt	Molt alt
Alta	Risc mitjà	Risc alt	Risc alt	Risc alt
Mitjana	Risc baix	Risc mitjà	Risc alt	Risc alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc alt

El resultat d'aquesta secció és un càlcul del risc per a cadascuna de les propietats de seguretat (confidencialitat, integritat, disponibilitat), així com una mesura de risc global (el màxim dels riscos anteriors).

6.5 Controls de seguretat

Un cop calculat el risc inicial, cal determinar quins controls (mesures per millorar la seguretat) s'han d'aplicar. Si el càlcul mostra un risc alt, cal aplicar controls de seguretat per reduir-lo; en cas contrari, això no és imprescindible. Ara bé, és recomanable aplicar uns controls mínims d'acord amb el risc estimat.

Els controls actuen sobre el risc de formes diverses: evitant que un incident es produeixi; reduint l'impacte d'un l'incident, si es produeix; facilitant la recuperació en cas d'incident; etc. Podem trobar diferents llistes de controls. Aquí fem ús dels controls de l'ENS (Esquema Nacional de Seguretat).

A l'hora de determinar els controls de seguretat a aplicar, l'ENS només té en compte l'impacte. És a dir, la necessitat i la intensitat amb què cal aplicar un control depèn de l'impacte associat a les diferents propietats de seguretat. A l'ENS es consideren les propietats següents: confidencialitat (C), integritat (I), disponibilitat (D), autenticitat (A) i traçabilitat (T). També es considera la categoria del sistema, que és el màxim dels impactes de les propietats anteriors. En el nostre cas, ens hem limitat a la confidencialitat (C), la integritat (I), la disponibilitat (D) i el sistema.

El nostre objectiu és reduir el risc, i això es pot fer tant reduint l'impacte com la probabilitat. En general, els controls es classifiquen segons l'objectiu que tenen. Els controls preventius i dissuasius redueixen la probabilitat d'un incident, mentre que els controls correctius, de

recuperació i compensatoris en redueixen l'impacte. A l'ENS, els controls són força complexos i, en general, tenen efecte tant sobre l'impacte com sobre la probabilitat.

Com a guia a l'hora de decidir els controls necessaris, proposem els dos criteris següents:

- Per reduir l'impacte, aplicarem els controls d'acord amb les dimensions de seguretat que es veuen afectades pel control. La intensitat amb què cal aplicar el control s'ha de determinar d'acord amb l'impacte de la dimensió de seguretat.

- Per reduir la probabilitat, cal reduir el nombre de preguntes de la secció 6.3 que tenen resposta afirmativa.

  La millor manera de fer-ho és evitar la casuística a què fa referència la pregunta. Per exemple, una resposta afirmativa a la pregunta "Q2. Es fa alguna part del tractament a través d'internet?" es pot transformar en negativa, si desconnectem el sistema d'internet i forcem que el tractament es faci in situ.

  Quan no sigui possible evitar completament la casuística de les preguntes, cal aplicar controls de seguretat per reduir la probabilitat que hi hagi un atac. La taula següent mostra els controls que poden tenir efecte sobre cadascuna de les preguntes de la secció 6.3.

Control	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
[org.1]			x	x											
[org.2]						x	x								
[org.3]												x			
[org.4]					x	x	x	x		x					
[op.pl.2]			x	x											
[op.pl.3]			x												
[op.pl.4]			x												
[op.pl.5]			x												
[op.acc.1]					x					x					
[op.acc.2]					x					x					
[op.acc.3]						x				x					
[op.acc.4]					x					x					
[op.acc.5]					x					x					
[op.acc.6]					x				x						
[op.acc.7]		x							x						
[op.exp.1]					x	x									
[op.exp.2]			x												
[op.exp.3]			x												
[op.exp.4]				x											
[op.exp.5]				x											

Control	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
[op.exp.6]		x	x	x				x							
[op.exp.7]				x											
[op.exp.8]									x						
[op.exp.9]				x											
[op.exp.10]									x						
[op.exp.11]			x												
[op.ext.1]											x				
[op.ext.2]											x				
[op.ext.3]															
[op.cont.1]			x								x				
[op.cont.2]			x	x											
[op.cont.3]			x	x											
[op.mon.1]	x	x		x	x				x						
[op.mon.2]			x												
[mp.if.1]					x				x						
[mp.if.2]					x				x						
[mp.if.3]					x										
[mp.if.4]					x										
[mp.if.5]					x										
[mp.if.5]					x										
[mp.if.6]					x										
[mp.if.7]					x				x						
[mp.if.8]					x										
[mp.per.1]						x	x					x			
[mp.per.2]						x						x			
[mp.per.3]												x			
[mp.per.4]												x			
[mp.per.5]												x			
[mp.eq.1]					x										
[mp.eq.2]				x											
[mp.eq.3]			x		x										
[mp.eq.4]			x		x										
[mp.com.1]	x	x													
[mp.com.2]	x	x													
[mp.com.3]	x	x													
[mp.com.4]				x											
[mp.com.5]	x	x													
[mp.si.1]					x										
[mp.si.2]					x										
[mp.si.3]					x										
[mp.si.4]					x										
[mp.si.5]					x										

Control	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
[mp.sw.1]			x												
[mp.sw.2]			x												
[mp.info.2]						x				x					
[mp.info.3]	x	x			x										
[mp.info.4]			x												
[mp.info.5]									x						
[mp.info.6]						x				x					
[mp.info.7]				x	x										
[mp.s.1]		x				x									
[mp.s.2]	x	x													
[mp.s.3]	x	x													
[mp.s.4]	x														

Aquests criteris constitueixen unes guies per ajudar a determinar els controls necessaris. Ara bé, a l'hora de calcular el risc residual, cal justificar l'efecte que tenen aquests controls sobre l'impacte i sobre la probabilitat.

6.5.1 Política de seguretat [org.1] (sistema)

La política de seguretat és un document d'alt nivell que estableix els principis bàsics de seguretat en una organització.

Nivell: baix, mitjà, alt

La política de seguretat ha d'establir de forma clara, com a mínim, el següent:

- Els objectius de l'organització.
- El marc legal en què es desenvolupen les activitats.
- Els rols i les funcions de seguretat, que han de definir els deures i responsabilitats de cadascú i el procediment per a la designació i renovació.
- Comitès de coordinació de la seguretat (membres i responsabilitats).
- Directrius per a l'estructuració de la informació de seguretat.

6.5.2 Normativa de seguretat [org.2] (sistema)

Risc: baix, mitjà, alt

Cal disposar d'una sèrie de documents que descriguin:

- L'ús correcte d'equips, serveis i instal·lacions.

- Què es considera ús inapropiat.
- Les responsabilitats del personal respecte del compliment o violació d'aquestes normes (drets, deures i mesures disciplinàries).

6.5.3 Procediments de seguretat [org.3] (sistema)

Risc: baix, mitjà, alt

Cal disposar d'una sèrie de documents que descriguin:

- Com desenvolupar les tasques habituals.
- Qui ha de fer cada tasca.
- Com identificar comportaments anòmals i informar-ne.

6.5.4 Procés d'autorització [org.4] (sistema)

Risc: baix, mitjà, alt

Cal establir un procés formal d'autoritzacions que abasti tots els elements del sistema:

- Ús de les instal·lacions (habituals i alternatives).
- Entrada d'equips en producció.
- Entrada d'aplicacions en producció.
- Establiment d'enllaços amb altres sistemes.
- Utilització de mitjans de comunicació (habituals i alternatius).
- Utilització de suports d'informació.
- Utilització d'equips mòbils.

6.5.5 Arquitectura de seguretat [op.pl.2] (sistema)

Risc: baix, mitjà, alt

La seguretat del sistema ha de ser objecte de plantejament integral, com a mínim, en:

- Documentació de les instal·lacions (àrees i punts d'accés).
- Documentació del sistema (equips, xarxes i punts d'accés al sistema).
- Esquema de línies de defensa (tallafocs, DMZ, tecnologies per prevenir vulnerabilitats).
- Sistema d'identificació i autenticació.
- Controls tècnics interns.

6.5.6 Adquisició de nous components [op.pl.3] (sistema)

Risc: baix, mitjà, alt

Cal establir un procediment formal per planificar l'adquisició de nous components del sistema, que ha de:

- Ser conforme a les conclusions de l'anàlisi de riscos.
- Seguir l'arquitectura de seguretat.
- Preveure les necessitats tècniques, de formació i de finançament.

6.5.7 Dimensionament [op.pl.4] (D)

Risc: mitjà, alt

Estudi previ a la posada en marxa del sistema, que inclogui les necessitats de:

- Tractament.
- Emmagatzematge.
- Comunicació.
- Personal (quantitat i qualificació).
- Instal·lacions i mitjans auxiliars.

6.5.8 Components certificats [op.pl.5] (sistema)

Risc: alt

Cal utilitzar sistemes, productes o equips amb funcionalitats de seguretat certificades per entitats independents de solvència reconeguda.

6.5.9 Identificació [op.acc.1] (sistema[11])

Risc: baix, mitjà, alt

Cal assignar un identificador singular a cada entitat que accedeixi al sistema.

[11] A l'ENS, les propietats són AT.

6.5.10 Requeriments d'accés [op.acc.2] (ICAT)

Risc: baix, mitjà, alt

- Només poden utilitzar els recursos del sistema les entitats que disposen de drets d'accés suficients.
- Els drets d'accés s'han d'establir d'acord amb el responsable de cada recurs i seguint la política i la normativa de seguretat.
- Cal controlar, particularment, l'accés als components del sistema i als fitxers de configuració.

6.5.11 Segregació de funcions i tasques [op.acc.3] (ICAT)

Risc: mitjà, alt

Necessitat de concurrència de dues o més persones per fer tasques crítiques.

6.5.12 Procés de gestió de drets d'accés [op.acc.4] (ICAT)

Risc: baix, mitjà, alt

Els drets d'accés de cada persona usuària s'han d'assignar d'acord amb:

- Mínim privilegi.
- Necessitat de conèixer.
- Únicament el personal competent pot modificar els drets d'accés, d'acord amb els criteris establerts pel responsable.

6.5.13 Mecanisme d'autenticació [op.acc.5] (ICAT)

Risc: baix, mitjà, alt

- S'accepta qualsevol mecanisme d'autenticació.
- Les paraules de pas han d'estar sota el control exclusiu de la persona usuària.
- La persona usuària ha de reconèixer la recepció i acceptar les obligacions (custòdia diligent i informació immediata, en cas de pèrdua).
- Els autenticadors s'han de renovar periòdicament, d'acord amb la política de l'organització.
- Els autenticadors s'han retirar i deshabilitar quan l'entitat (persona, equip o
- procés) acaba la seva relació amb el sistema.

Risc: mitjà, alt

- No es recomana utilitzar claus de pas.
- Es recomana utilitzar dispositius físics (tokens), lògics (certificats digitals) o biomètrics.
- Si s'empren paraules de pas, cal aplicar polítiques rigoroses de qualitat i renovació.

Risc: alt

- Els autenticadors s'han de suspendre automàticament, si no s'utilitzen.
- No s'admeten paraules de pas.
- S'exigeix l'ús de dispositius físics o biometria.
- Cal que els dispositius físics facin ús d'algorismes acreditats.
- Cal utilitzar preferentment productes certificats.

6.5.14 Accés local [op.acc.6] (ICAT)

Un accés local és el que es fa des de dins de les pròpies instal·lacions.

Risc: baix, mitjà, alt

- Cal evitar els atacs que, tot i no donar accés, poden revelar informació del sistema.
- Cal blocar l'accés després d'un nombre fixat d'intents fallits.
- Cal registrar els intents d'accés (amb èxit i fallits).
- En el moment de l'accés, el sistema ha d'informar la persona usuària de les seves obligacions.

Risc: mitjà, alt

- S'ha d'informar la persona usuària de l'últim accés amb la seva identitat.

Risc: alt

- L'accés s'ha de limitar per data i hora.
- Cal definir punts on la persona usuària ha de renovar l'autenticació.

6.5.15 Accés remot [op.acc.7] (ICAT)

Un accés remot és el que es fa des de fora de les instal·lacions de l'organització.

Risc: baix, mitjà, alt

- Cal protegir l'accés de la mateixa manera que es fa a l'accés local.
- Cal protegir les comunicacions.

Risc: mitjà, alt

- Cal establir una política que especifiqui quines tasques es poden fer remotament i cal autoritzar la persona usuària prèviament.

6.5.16 Inventari d'actius [op.exp.1] (sistema)

Risc: baix, mitjà, alt

- S'ha de mantenir un registre dels actius del sistema que en descriu la tipologia i n'identifica el responsable.

6.5.17 Configuració de seguretat [op.exp.2] (sistema)

Risc: baix, mitjà, alt

Els equips s'han de configurar abans que comencin a operar, de manera que:

- S'esborrin comptes i paraules de pas estàndard.
- S'apliqui la regla de la mínima funcionalitat.
- S'apliqui la regla de seguretat per defecte.

6.5.18 Gestió de la configuració [op.exp.3] (sistema)

Risc: mitjà, alt

La configuració del sistema s'ha de gestionar de forma contínua, de manera que:

- En tot moment es manté la regla de funcionalitat mínima.
- En tot moment es manté la regla de seguretat per defecte.
- El sistema s'adapta a les noves necessitats.
- El sistema reacciona a les vulnerabilitats reportades.
- El sistema reacciona a incidències.

6.5.19 Manteniment [op.exp.4] (sistema)

Risc: baix, mitjà, alt

- Cal respectar les especificacions dels fabricants pel que fa a la instal·lació i el manteniment dels sistemes.
- Cal fer un seguiment continu dels comunicats de defectes.
- Cal disposar d'un sistema per analitzar, prioritzar i aplicar les actualitzacions
- de seguretat.

6.5.20 Gestió de canvis [op.exp.5] (sistema)

Risc: mitjà, alt

S'ha de mantenir un control continu dels canvis realitzats al sistema:

- Tots els canvis anunciats pel fabricant s'han d'analitzar, per determinar-ne la conveniència.
- Abans d'aplicar canvis a producció, s'han de comprovar en un equip que no estigui en producció.
- Els canvis s'han de planificar, per reduir l'impacte sobre la prestació de serveis.
- Els canvis que suposin un risc alt s'han d'aprovar explícitament.

6.5.21 Protecció contra codi maliciós [op.exp.6] (sistema)

Risc: baix, mitjà, alt

- Cal disposar de mecanismes de prevenció i reacció contra codi maliciós.

6.5.22 Gestió d'incidències [op.exp.7] (sistema)

Risc: mitjà, alt

Es disposarà d'un procés per fer front als incidents de seguretat.

- Procediment de notificació.
- Registre d'evidències

6.5.23 Registre de l'activitat de les persones usuàries [op.exp.8] (sistema[12])

Risc: alt

Cal registrar totes les activitats de les persones usuàries del sistema, de manera que:

- Indiqui qui fa una activitat, quan la fa i sobre quines dades.
- Inclogui l'activitat de les persones usuàries, d'operadors i administradors.
- Hi constin les activitats fetes i els intents fallits.

6.5.24 Registre de la gestió d'incidències [op.exp.9] (sistema)

Risc: mitjà, alt

Cal registrar totes les actuacions relacionades amb la gestió d'incidències:

- L'informe inicial, les actuacions i les modificacions al sistema.
- Les evidències que puguin sustentar o fer front a una demanda judicial.
- Com a resultat de l'anàlisi d'incidències, s'han de revisar els esdeveniments auditables.

6.5.25 Protecció dels registres d'activitat [op.exp.10] (sistema[13])

Risc: alt

Cal protegir els registres del sistema, de manera que:

- S'ha de determinar el període de retenció dels registres.
- Se n'ha d'assegurar la data i hora.
- El personal no autoritzat no ha de poder modificar els registres.
- Les còpies de seguretat, si n'hi ha, han de tenir els mateixos requeriments.

6.5.26 Protecció de les claus criptogràfiques [op.exp.11] (sistema)

Les claus criptogràfiques s'han de protegir durant tot el seu cicle de vida: generació, transport al punt d'explotació, custòdia durant l'explotació, arxiu i destrucció.

---

[12] A l'ENS la propietat és T.

[13] A l'ENS la propietat és T.

Risc: baix, mitjà, alt

- Els mitjans de generació han d'estar aïllats dels d'explotació.
- Les claus arxivades han d'estar en suports aïllats dels d'explotació.

Risc: mitjà, alt

- Cal emprar eines certificades (algorismes, programes, dispositius).

6.5.27 Contractació i acords de nivell de servei [op.ext.1] (sistema)

Risc: mitjà, alt

- Abans d'emprar recursos externs, cal establir contractualment les característiques del servei i les responsabilitats de les parts. En particular, cal establir la qualitat mínima del servei i les conseqüències d'un incompliment.

6.5.28 Gestió diària [op.ext.2] (sistema)

Risc: mitjà, alt

Per a la gestió diària del sistema, cal:

- Un sistema per mesurar el compliment de les obligacions de servei.
- Mecanismes i coordinació per fer les tasques de manteniment dels sistemes afectats per l'acord.
- Mecanismes i coordinació en cas d'incidències.

6.5.29 Mitjans alternatius [op.ext.3] (D)

Risc: alt

Cal preveure que el servei estigui proveït amb mitjans alternatius, si el servei contractat no està disponible. El servei alternatiu ha d'oferir les mateixes garanties.

6.5.30 Continuïtat del servei [op.cont.1] (D)

Risc: mitjà, alt

Cal fer una anàlisi del següent:

- Requeriments de disponibilitat de cada servei, segons el seu impacte.
- Elements crítics per a cada servei.

6.5.31 Pla de continuïtat [op.cont.2] (D)

Risc: alt

Cal establir un pla de continuïtat en cas d'interrupció dels serveis oferts amb els mitjans habituals:

- S'han d'identificar funcions, responsabilitats i activitats a realitzar.
- Cal preveure mitjans alternatius per continuar oferint els serveis.
- Tots els mitjans alternatius han d'estar planificats i materialitzats en contractes o acords amb els proveïdors corresponents.
- Totes les persones afectades han de rebre formació específica.
- El pla de continuïtat s'ha d'integrar amb altres plans de continuïtat en matèries alienes a la seguretat.

6.5.32 Proves periòdiques [op.cont.3] (D)

Risc: alt

Cal fer proves periòdiques per detectar i corregir els errors o les deficiències que hi pugui haver al pla de continuïtat.

6.5.33 Detecció d'intrusions [op.mon.1] (sistema)

Risc: alt

Cal disposar d'eines de detecció i prevenció d'intrusions.

6.5.34 Sistema de mètriques [op.mon.2] (sistema)

Risc: alt

Cal establir un conjunt d'indicadors que mesuri la seguretat del sistema en els aspectes següents:

- Grau d'implantació de les mesures de seguretat.
- Eficàcia i eficiència de les mesures de seguretat.
- Impacte dels incidents de seguretat.

6.5.35 Àrees separades i control d'accés [mp.if.1] (sistema)

Risc: baix, mitjà, alt

- L'equipament s'ha d'instal·lar en àrees separades específiques per a la seva funció.
- Cal controlar l'accés a les àrees indicades, de manera que només s'hi pugui accedir per les entrades previstes i vigilades.

6.5.36 Identificació de les persones [mp.if.2] (sistema)

Risc: baix, mitjà, alt

- Cal identificar totes les persones que accedeixen als locals on hi hagi equipament del sistema informàtic.
- Cal registrar l'entrada i la sortida de persones.

6.5.37 Condicionament dels locals [mp.if.3] (sistema)

Risc: baix, mitjà, alt

Els locals on s'ubiquen els sistemes d'informació i els seus components han de disposar d'elements adequats per fer eficaç el funcionament de l'equipament instal·lat.

- Condicions de temperatura i humitat.
- Protecció contra les amenaces identificades a l'anàlisi de risc.
- Protecció del cablejat contra incidents fortuïts o deliberats.

6.5.38 Energia elèctrica [mp.if.4] (D)

Risc: baix

Els locals on s'ubiquen els sistemes d'informació i els seus components han de disposar de l'energia elèctrica necessària per funcionar, de manera que es garanteixi:

- El subministrament d'energia elèctrica.
- El funcionament correcte dels llums d'emergència.

Risc: baix, mitjà, alt

En cas de fallada del subministrament general, cal garantir el subministrament elèctric dels sistemes, amb el temps suficient per fer una apagada ordenada i salvaguardant la informació.

6.5.39 Protecció contra incendis [mp.if.5] (D)

Risc: baix, mitjà, alt

Els locals on s'ubiquen els sistemes d'informació i els seus components s'han de protegir contra incendis fortuïts o deliberats.

6.5.40 Protecció contra inundacions [mp.if.6] (D)

Risc: mitjà, alt

Els locals on s'ubiquen els sistemes d'informació i els seus components s'han de protegir contra incidents fortuïts o deliberats causats per l'aigua.

6.5.41 Registre d'entrada i de sortida d'equipament [mp.if.7] (sistema)

Risc: baix, mitjà, alt

S'ha de mantenir un registre detallat de l'entrada i la sortida d'equipament, que inclogui la identificació de la persona que autoritza el moviment.

6.5.42 Instal·lacions alternatives [mp.if.8] (D)

Risc: alt

Cal garantir que hi ha instal·lacions alternatives per poder treballar, i que estan disponibles, si les habituals no estan disponibles. Les instal·lacions alternatives han de disposar de les mateixes garanties que les habituals.

6.5.43 Caracterització del lloc de treball [mp.per.1] (sistema)

Risc: mitjà, alt

- Cal definir les responsabilitats relacionades amb la seguretat en cada lloc de treball.
- Cal definir les condicions que han de satisfer les persones que ocupen cada lloc de treball (en particular, respecte de la confidencialitat).
- Cal tenir en compte les condicions anteriors en la selecció del personal, inclosa la verificació de la seva vida laboral, formació i altres dades.

6.5.44 Deures i obligacions [mp.per.2] (sistema)

Risc: baix, mitjà, alt

Cal informar cada persona que treballa en el sistema dels deures i les responsabilitats en matèria de seguretat:

- Les mesures disciplinàries.
- Les obligacions tant el període de desenvolupament de la feina com en el cas de finalització o trasllat.
- El deure de confidencialitat respecte de les dades a què té accés.

Per al personal contractat a través d'un tercer, cal establir:

- Els deures i les obligacions del personal.
- Els deures i les obligacions de cada part.
- El procediment per resoldre incidents relacionats amb l'incompliment de les obligacions.

6.5.45 Conscienciació [mp.per.3] (sistema)

Risc: baix, mitjà, alt

Cal fer les accions necessàries per conscienciar regularment el personal respecte del seu paper perquè la seguretat del sistema assoleixi el nivell exigit. En particular, cal recordar:

- La normativa relativa al bon ús dels sistemes.
- La identificació d'incidents, activitats o comportaments sospitosos que cal reportar.
- El procediment per informar d'incidències de seguretat.

6.5.46 Formació [mp.per.4] (sistema)

Risc: baix, mitjà, alt

Cal formar regularment el personal en totes les matèries necessàries per al desenvolupament de les seves funcions, en particular respecte del següent:

- Configuració del sistema.
- Detecció i reacció a incidents.
- Gestió de la informació en qualsevol suport. Cal abastar, com a mínim, les activitats següents: emmagatzematge, transferència, còpia, distribució i destrucció.

6.5.47 Personal alternatiu [mp.per.5] (D)

Risc: alt

Cal garantir la disponibilitat d'altres persones que puguin fer-se càrrec de les funcions, si el personal habitual no està disponible. El personal alternatiu ha d'estar sotmès a les mateixes garanties que l'habitual.

6.5.48 Lloc de treball buidat [mp.eq.1] (sistema)

Risc: baix, mitjà, alt

S'ha d'exigir que els llocs de treball romanguin buits, sense més material a la taula que el necessari per a l'activitat que s'està fent en cada moment.

Risc: mitjà, alt

El material s'ha de desar en un lloc tancat.

6.5.49 Bloqueig del lloc de treball [mp.eq.2] (sistema)

Risc: mitjà, alt

El lloc de treball s'ha de bloquejar al cap d'un temps d'inactivitat i cal requerir l'autenticació de la persona usuària per continuar l'activitat.

Risc: alt

Passat un temps, superior a l'anterior, s'han de tancar les sessions obertes des del lloc de treball.

6.5.50 Protecció de portàtils [mp.eq.3] (sistema)

Risc: baix, mitjà, alt

Els equips que abandonen les instal·lacions s'han de protegir adequadament:

- Cal fer un inventari dels equips portàtils, amb la identificació de la persona responsable i control regular que els equips estan sota el seu control.
- Cal establir un canal per informar de pèrdues o sostraccions.
- Cal que hi hagi un sistema de protecció perimetral, que minimitzi la visibilitat exterior i controli l'accés quan l'equip es connecti a xarxes, en particular a xarxes públiques.
- Cal evitar, en la mesura que sigui possible, que l'equip tingui claus d'accés remot a l'organització.

Risc: alt

- L'equip ha de disposar de detectors de violació que permetin saber si l'equip ha estat manipulat.
- La informació de nivell alt que té emmagatzemada s'ha de xifrar.

6.5.51 Mitjans alternatius [mp.eq.4] (D)

Risc: mitjà, alt

- Cal garantir la disponibilitat de mitjans alternatius de tractament de la informació, si els habituals fallen. Aquests mitjans alternatius han d'estar subjectes a les mateixes garanties de protecció.
- Cal establir un temps màxim perquè els equips alternatius entrin en funcionament.

6.5.52 Perímetre segur [mp.com.1] (sistema)

Risc: baix, mitjà, alt

- Cal disposar d'un tallafocs que separi la xarxa interna de l'exterior. Tot el trànsit ha de passar a través del tallafocs, que només ha de permetre els fluxos prèviament autoritzats.

Risc: alta

- El tallafocs ha de constar de dos o més equips de diferents fabricants en cascada.
- Cal disposar de sistemes redundants.

6.5.53 Protecció de la confidencialitat [mp.com.2] (C)

Risc: mitjà, alt

- Cal utilitzar una VPN, quan la comunicació passi per fora del domini de seguretat.
- Cal utilitzar algorismes acreditats pel CCN.

Risc: alt

- Preferentment, cal utilitzar dispositius de maquinari per establir i utilitzar la VPN.
- Preferentment, cal utilitzar productes certificats.

6.5.54 Protecció de l'autenticitat i de la integritat [mp.com.3] (IA)

Risc: baix, mitjà, alt

- Cal garantir l'autenticitat de l'altre extrem d'un canal de comunicació, abans d'intercanviar informació.
- Cal prevenir atacs actius i garantir que, com a mínim, es detectin. Es consideren atacs actius: l'alteració de la informació en trànsit, la introducció d'informació espúria i el segrest de la sessió per una tercera part.

Risc: mitjà, alt

- Cal utilitzar una VPN, quan la comunicació passi per fora del domini de seguretat.
- Cal utilitzar algorismes acreditats pel CCN.

Risc: alt

- S'ha de valorar positivament l'ús de dispositius de maquinari a l'hora d'establir la VPN.
- Preferentment, cal utilitzar productes certificats.

6.5.55 Segregació de xarxes [mp.com.4] (sistema)

La segregació de xarxes limita la propagació dels incidents de seguretat, que queden restringits a l'entorn on tenen lloc.

Risc: alt

La xarxa s'ha de segmentar, de manera que hi hagi:

- Control d'entrada de les persones usuàries a cada segment.
- Control de sortida de la informació de cada segment.
- Els punts d'interconnexió (físic o lògic) han d'estar particularment assegurats, mantinguts i monitoritzats.

6.5.56 Mitjans alternatius [mp.com.5] (D)

Risc: alt

Cal garantir que hi ha mitjans de comunicació alternatius si els habituals fallen, i que estan disponibles. Cal que els mitjans alternatius:

- Estiguin subjectes a les mateixes garanties de protecció que els habituals.
- Garanteixin un temps màxim d'entrada en funcionament.

6.5.57 Etiquetat [mp.si.1] (C)

Risc: baix, mitjà, alt

- Els suports d'informació s'han d'etiquetar de manera que, sense revelar-ne el contingut, s'indiqui el nivell de seguretat de la informació continguda.
- Les persones usuàries han d'estar capacitats per entendre el significat de les etiquetes.

6.5.58 Criptografia [mp.si.2] (IC)

Aquesta mesura s'aplica, en particular, a tots els dispositius extraïbles (CD, DVD, discs USB i altres d'anàlegs).

Risc: mitjà, alt

Cal aplicar mecanismes criptogràfics que garanteixin la integritat i la confidencialitat de la informació continguda.

Risc: alt

- Cal utilitzar algorismes acreditats pel CCN.
- Cal utilitzar, preferentment, productes certificats.

6.5.59 Custòdia [mp.si.3] (sistema)

Risc: baix, mitjà, alt

Cal aplicar la diligència i el control adequats als suports d'informació que estan sota la responsabilitat de l'organització.

- Cal garantir el control d'accés amb mesures físiques, lògiques o ambdues.
- Cal garantir que es respecten les exigències de manteniment del fabricant.

6.5.60 Transport [mp.si.4] (sistema)

Risc: baix, mitjà, alt

La persona responsable de sistemes ha de garantir que, mentre es desplacen, els dispositius estan sota control i que es compleixen els requisits de seguretat. Cal:

- Disposar d'un registre de sortida que identifiqui la persona transportista que rep el suport.
- Disposar d'un registre d'entrada que identifiqui la persona transportista que l'entrega.
- Disposar d'un procediment que compari entrades i sortides. Si es detecta algun incident, s'han d'activar les alarmes.
- Utilitzar mitjans criptogràfics d'acord amb [mp.si.2].
- Gestionar les claus d'acord amb [op.exp.11].

6.5.61 Esborrat i destrucció [mp.si.5] (C)

Risc: mitjà, alt

L'esborrat i destrucció del suport de la informació s'ha d'aplicar a qualsevol tipus d'equip susceptible d'emmagatzemar informació.

- Els suports que s'han de reutilitzar o lliurar a una altra organització han de ser objecte d'un esborrat segur.
- Cal destruir els suports de forma segura, quan la naturalesa del suport no permeti un esborrat segur i així ho requereixi el procediment associat a la informació continguda.

6.5.62 Desenvolupament d'aplicacions [mp.sw.1] (sistema)

Risc: mitjà, alt

- El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció. No hi ha d'haver eines o dades de desenvolupament a l'entorn de producció.
- Cal aplicar una metodologia de desenvolupament reconeguda, que:
  - Prengui en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
  - Tracti específicament les dades utilitzades a les proves.
  - Permeti la inspecció del codi font.
- Els elements següents han de ser part integral del disseny del sistema:
  - Mecanismes d'identificació i autenticació.
  - Mecanismes de protecció de la informació tractada.
  - La generació i el tractament de pistes d'auditoria.
- Les proves no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.

6.5.63 Acceptació i posada en servei [mp.sw.1] (sistema)

Risc: baix, mitjà, alt

Abans de passar a producció, cal comprovar que l'aplicació funciona correctament:

- S'ha de comprovar que es compleixen els criteris d'acceptació en matèria de seguretat i que no es deteriora la seguretat dels altres components del servei.
- Les proves s'han de fer en un entorn aïllat (preproducció).

- Les proves no s'han de fer amb dades reals, llevat que se'n pugui garantir la seguretat.

Risc: mitjà, alt

Abans de la posada en funcionament, cal fer les inspeccions següents:

- Anàlisi de vulnerabilitats.
- Proves de penetració.

Risc: alt

Abans de la posada en funcionament, cal:

- Fer una anàlisi de la coherència en la integració dels processos.
- Considerar l'oportunitat de fer una auditoria del codi font.

6.5.64 Qualificació de la informació [mp.info.2] (C)

Risc: baix, mitjà, alt

- Per qualificar la informació, cal tenir en compte la seva naturalesa.
- La política de seguretat ha d'establir la persona responsable de cada informació.
- La política de seguretat ha de contenir els criteris que determinen el nivell de seguretat requerit.
- Amb els criteris anteriors, la persona responsable de cada informació ha d'assignar a cada informació el nivell de seguretat requerit.
- La persona responsable de cada informació ha de tenir en exclusiva la potestat de modificar el nivell de seguretat requerit.

Risc: mitjà, alt

Cal redactar els procediments que descriguin com etiquetar i tractar la informació, segons el seu nivell de seguretat. En particular, com cal fer:

- El control d'accés.
- L'emmagatzematge.
- Les còpies.
- L'etiquetat del suports.
- La transmissió telemàtica.

6.5.65 Xifrat de la informació [mp.info.3] (C)

Risc: mitjà, alt

- La informació amb un nivell alt de confidencialitat s'ha de xifrar, durant l'emmagatzematge i la transmissió. Només ha d'estar en clar quan s'estigui utilitzant.
- L'ús de criptografia en les comunicacions s'ha de fer d'acord amb [mp.com.2].
- L'ús de criptografia en els suports s'ha de fer d'acord amb [mp.si.2].

6.5.66 Signatura electrònica [mp.info.4] (IA)

La signatura electrònica garanteix l'autenticitat de la persona signant i la integritat del contingut.

També és un mecanisme de prevenció del repudi.

Risc: baix

Es pot utilitzar qualsevol mitjà de signatura electrònica.

Risc: mitjà, alt

Els mitjans de signatura electrònica han de ser proporcionals a la qualificació de la informació tractada. En qualsevol cas, cal utilitzar:

- Algorismes acreditats pel CCN.
- Certificats reconeguts, preferentment.
- Dispositius segurs de signatura, preferentment.

S'ha de garantir la verificació i la validació de la signatura. Amb aquesta finalitat:

- S'ha d'adjuntar a la signatura tota la informació pertinent: certificats i dades de verificació i de validació.
- S'ha de protegir la signatura amb un segell temporal.
- L'organisme que recull els documents signats ha de verificar i validar la signatura, en el moment de recepció.

Risc: alt

- Cal utilitzar certificats reconeguts.
- Cal utilitzar dispositius segurs de creació de signatures.
- Cal utilitzar, preferentment, productes certificats.

6.5.67 Segells temporals [mp.info.5] (T)

Risc: alt

Els segells temporals eviten la possibilitat de repudi posterior:

- S'han d'aplicar a la informació que pugui ser utilitzada com a evidència electrònica en el futur.
- Les dades per verificar la data s'han de tractar amb la mateixa seguretat que la informació.
- Cal utilitzar productes certificats o serveis externs admesos.

6.5.68 Neteja de documents [mp.info.6] (C)

Risc: baix, mitjà, alt

El procés de neteja de documents ha d'eliminar tota la informació addicional que hi hagi en camps ocults, meta-dades, comentaris o revisions anteriors, llevat de si aquesta informació és pertinent a la persona receptora.

Aquesta mesura és especialment rellevant quan el document es difon àmpliament.

6.5.69 Còpies de seguretat [mp.info.7] (D)

Risc: mitjà, alt

Cal fer còpies de seguretat que permetin recuperar dades perdudes accidentalment o intencionadament.

Les còpies han de tenir la mateixa seguretat que les dades inicials. En particular, cal considerar la necessitat que estiguin xifrades.

Les còpies han de contenir:

- Informació de treball de l'organització.
- Les aplicacions en explotació, inclosos els sistemes operatius.
- Les dades de configuració, serveis, aplicacions, equips i altres d'anàlegs.
- Les claus utilitzades per preservar la confidencialitat de la informació.

6.5.70 Protecció del correu electrònic [mp.s.1] (sistema)

Risc: baix, mitjà, alt

- La informació distribuïda per correu electrònic s'ha de protegir, tant al cos com als annexos.
- S'ha de protegir la informació d'encaminament de missatges i establiment de connexions.
- S'ha de protegir l'organització de problemes que es materialitzen per correu electrònic: correu brossa, programari maliciós (virus, cucs, etc.), codi.
- S'han d'establir normes per l'ús apropiat del correu electrònic. Aquestes normes han de tenir: limitacions d'ús i activitats de formació i conscienciació.

6.5.71 Protecció de serveis i aplicacions web [mp.s.2] (sistema)

Risc: baix, mitjà, alt

Quan la informació tingui algun tipus de control d'accés, cal garantir la impossibilitat d'accedir a la informació sense autenticar-se. En particular, cal:

- Evitar que el servidor ofereixi accés als documents per vies alternatives.
- Prevenir atacs de manipulació d'URL.
- Prevenir atacs de manipulació de galetes.
- Prevenir atacs d'injecció de codi.
- Prevenir els intents d'escalada de privilegis.
- Prevenir els atacs de XSS.
- Prevenir els atacs de manipulació de servidors intermedis (proxy) i de memòria cau (caché).

6.5.72 Protecció contra la denegació de servei [mp.s.3] (D) (impacte, probabilitat)

Risc: mitjà, alt

S'han d'establir mesures preventives i reactives contra els atacs de denegació de servei:

- Dotar el sistema de la capacitat suficient per atendre la càrrega prevista.
- Desplegar tecnologies per prevenir els atacs coneguts.

Risc: alt

- Cal establir un sistema de detecció dels atacs de denegació de servei.
- Cal establir procediments de reacció als atacs, inclosa la comunicació amb el proveïdor de comunicacions.
- Cal impedir que es llancin atacs des de les pròpies instal·lacions.

6.5.73 Mitjans alternatius [mp.s.9] (D) (impacte)

Risc: alt

Cal garantir que hi ha mitjans alternatius si els habituals fallen, i que estan disponibles. Aquests mitjans alternatius han de tenir les mateixes garanties de protecció que els habituals.

6.6 Càlcul del risc residual

Un cop establerts els controls de seguretat, cal determinar com afecten al risc. En general, els controls de seguretat es classifiquen segons l'objectiu que tenen: preventiu, detectiu, correctiu, dissuasiu, de recuperació i compensatori. A l'hora de calcular el risc, l'efecte dels controls es tradueix en una reducció de l'impacte o de la probabilitat d'un incident.

A la secció anterior hem donat unes pautes per seleccionar els controls a aplicar, d'acord amb l'impacte i la probabilitat. Aquestes pautes són merament indicatives i no es tradueixen en una reducció directa de l'impacte o de la probabilitat d'un incident. És el responsable del tractament qui ha de decidir quins controls cal aplicar i justificar els efectes que aquests controls tenen sobre l'impacte i la probabilitat.

El risc residual es calcula a partir de l'impacte residual i la probabilitat residual, utilitzant la taula de la secció 4.6. Si el risc residual és alt, cal proposar nous controls per reduir- lo. Si no és possible reduir-lo, abans d'iniciar el tractament cal consultar l'autoritat de protecció de dades competent sobre la seva idoneïtat.