VERSIÓ FINAL

ENQUESTA SOBRE LA NOTIFICACIÓ DE VIOLACIONS DE SEGURETAT

(GPEN Privacy Sweep 2019)

Índex

INTRODUCCIÓ

L'Autoritat Catalana de Protecció de Dades (APDCAT) com a membre del "Global Privacy Enforcement Network (GPEN)", una xarxa global de protecció de dades de la qual formen part autoritats de protecció de dades de diferents països europeus i de la resta del món, ha participat en la iniciativa "2019 GPEN Sweep" relacionada amb la gestió de les notificacions de violacions de seguretat.

Tot i que l'APDCAT ja disposa d'informació directa sobre les violacions de seguretat efectuades al seu àmbit d'actuació, participar en aquest projecte ha permès a l'APDCAT conèixer, des del punt de vista de les entitats afectades, la situació actual del compliment d'aquesta obligació entre les entitats incloses al seu àmbit d'actuació i detectar els aspectes que resulten més problemàtics per les entitats afectades.

El procediment seguit ha estat la realització d'una enquesta a un centenar d'entitats, seleccionades bé per pertànyer a una determinada categoria (departaments de la Generalitat, universitats i col·legis professionals) o bé mitjançant una mostra aleatòria (ajuntaments de menys de 50.000 habitants).

L'enquesta s'ha dut a terme durant la setmana del 16 al 20 de setembre de 2019. De les 100 entitats seleccionades, 57 han contestat l'enquesta, bé per via telefònica (11 entitats), bé a través d'un correu electrònic (46 entitats) tramès durant la setmana de realització de l'enquesta. La majoria d'entitats comptava amb un delegat de protecció de dades designat que ha pogut respondre les preguntes. Ara bé, en alguns casos concrets no s'ha pogut contactar amb el delegat de protecció de dades, per no tenir-lo designat o perquè no estava disponible.

S'ha de fer notar que en molts dels ajuntaments seleccionats l'enquesta s'ha fet a través del seu delegat de protecció de dades extern: 26 dels ajuntaments seleccionats tenien delegada aquesta funció en la diputació provincial respectiva i d'altres la tenien delegada en empreses externes.

En aquest sentit, cal recordar que en l'àmbit de les administracions públiques la designació del delegat de protecció de dades és obligatòria i que una de les funcions

que té atribuïdes el delegat de protecció de dades és precisament la d'actuar com a interlocutor amb l'autoritat de protecció de dades (39.1.e)).

La mostra ha estat dividida en quatre sectors: els departaments de la Generalitat, les universitats catalanes, els col·legis professionals i els ajuntaments, aquests últims segmentats per número d'habitants. No s'ha pogut apreciar grans diferències entre uns i altres en les seves respostes, tot i que, els tipus d'entitats que han patit més violacions de seguretat han estat els de l'Administració de la Generalitat i les universitats, circumstància probablement relacionada amb les seves dimensions, front altres entitats que han participat a l'enquesta amb dimensions reduïdes.

D'altra banda, és important esmentar que només les entitats que han sofert violacions de seguretat en les dades durant aquest període han pogut respondre totes les preguntes perquè algunes d'elles estaven vinculades a la pregunta inicial "*quantes violacions de seguretat sofertes heu tingut aquest any*?".

A l'hora de fer l'enquesta s'ha remarcat a tots els participants que era totalment voluntària, que no implicava auditoria, ni inspecció, ni tenia finalitat sancionadora, sinó que el seu objectiu era simplement la recollida de dades globals sobre diferents aspectes lligats al compliment de l'obligació. Tot això, per tal de detectar en quins aspectes cal incidir per a millorar-ne el compliment.

ASPECTES ANALITZATS A L'ENQUESTA

En l'enquesta, que s'ha realitzat per via telefònica o a través de correu electrònic segons ha escollit cadascun dels ens afectats, s'han abordat els aspectes següents:

I. Notificació de violacions de seguretat a l'APDCAT

- **a.** Coneixement de l'obligació de notificar a l'APDCAT. Termini per notificar. Conseqüències de no notificar-ho.
- **b.** Número de violacions de seguretat.
- **c.** Número de notificacions a l'APDCAT i a altres autoritats.
- **d.** Procés de notificació.
- **e.** Criteri utilitzat per saber si notificar o no.
- **f.** Resposta rebuda per part de l'APDCAT. Accions empreses arran la resposta. Grau de satisfacció amb la resposta rebuda.
- **g.** Existència d'un protocol per notificar els incidents. Coneixement del càrrec que ha de notificar la violació. Existència d'instruccions a l'encarregat del tractament.

II. Comunicació a les persones afectades

- **a.** Número de comunicacions a les persones afectades.

III. Identificació del risc existent

- **a.** Establiment de criteris per avaluar el risc.
- **b.** Problemes per identificar el grau del risc.
- **c.** Anàlisi de supòsits pràctics sobre l'obligatorietat de notificar.

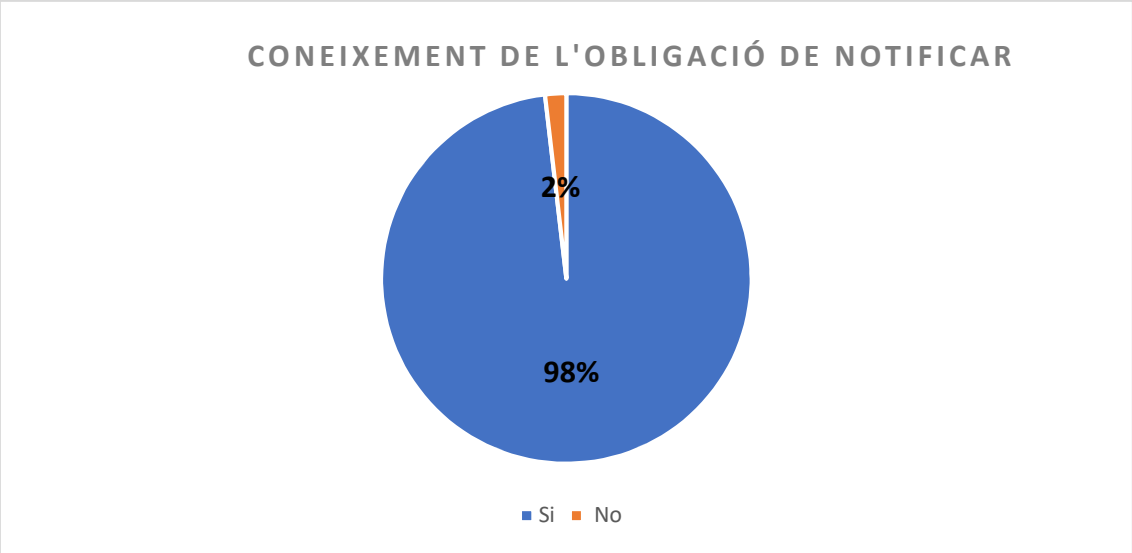
El text de les preguntes formulades s'adjunta a l'Annex 1.

I. Notificació de violacions de seguretat a l'APDCAT.

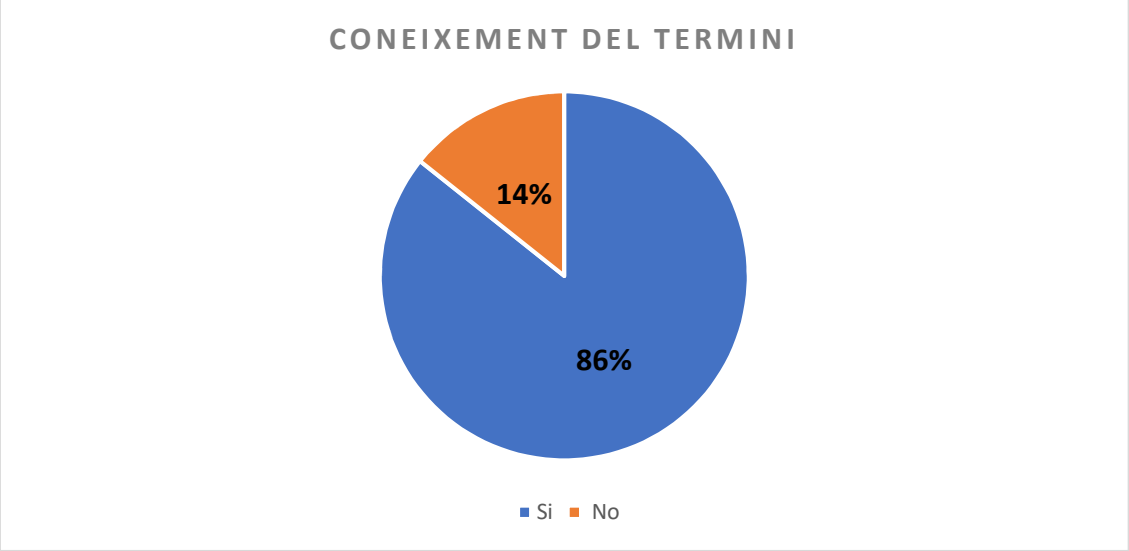
Coneixement de l'obligació de notificar a l'APDCAT. Termini per notificar. Conseqüències de no notificar-ho.

D'acord amb el que estableix l'article 33 del Reglament 2016/679, de 27 d'abril, general de Protecció de Dades (RGPD) si es produeix una violació de seguretat de les dades personals, les entitats responsables del tractament incloses en l'àmbit d'actuació de l'APDCAT han de notificar-la a aquesta Autoritat, sense dilació indeguda i, en un termini màxim de 72 hores des que n'hagin tingut constància. Això, tret que sigui improbable que la violació de seguretat constitueixi un risc pels drets i llibertats de les persones físiques.

Pràcticament la totalitat de les entitats enquestades coneixen l'obligació de notificar les violacions de seguretat. A aquests efectes, s'entén com a violació de seguretat que afecta les dades personals tota violació de seguretat que ocasiona la destrucció, pèrdua o alteració accidental o il·lícita de dades personals trameses, conservades o sotmeses a altres tractaments, o la comunicació o accessos no autoritzats a aquestes dades (article 4.12 RGPD).



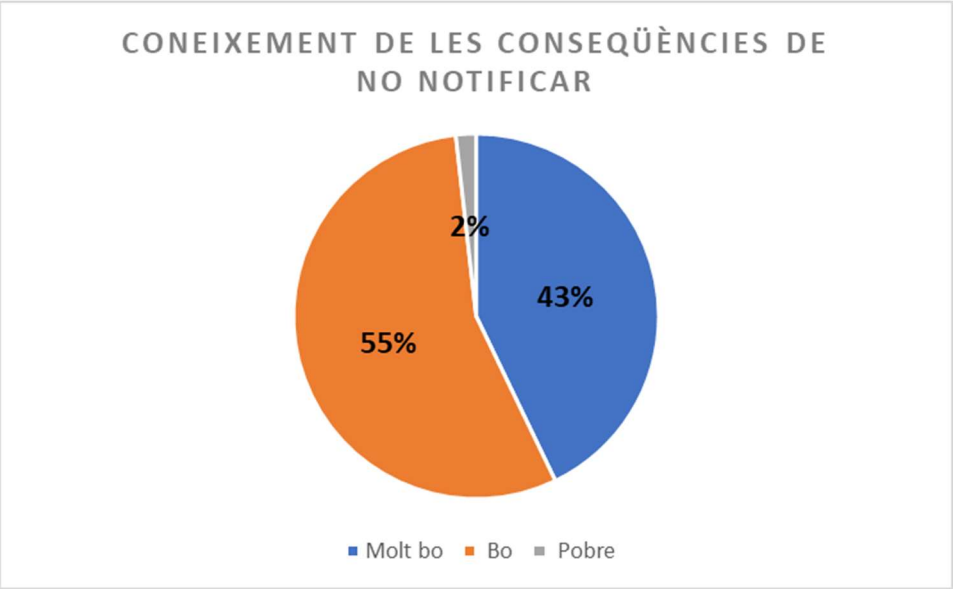
Malgrat que el coneixement de l'obligació de notificar les violacions és del 98%, el 14% de les entitats no han pogut concretar en quin termini s'ha de fer la notificació per no incórrer en una vulneració del Reglament General de Protecció de Dades (RGPD).



L'incompliment de l'obligació de notificar, pot tenir diferents conseqüències: pot dificultar la resposta a l'incident i si escau l'adopció de mesures correctores, impedir conèixer el criteri de l'autoritat pel que fa a la necessitat de comunicar la violació a les persones afectades o tenir fins i tot conseqüències sancionadores per no haver-se fet la notificació.

Del resultat de l'enquesta s'aprecia què el 98% de la mostra seleccionada coneix el fet que no notificar una violació de seguretat personals pot comportar conseqüències, en especial pel que fa a la possibilitat que constitueixi una infracció (infracció greu per manca de comunicació (art. 73.r) de la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)), ja sigui infracció lleu perquè la comunicació hagi incompleta, tardana o defectuosa (art. 74.m) LOPDGDD).

I un 43% manifesta tenir present que la manca de notificació a l'APDCAT no només pot tenir conseqüències en l'àmbit sancionador, sinó també altres conseqüències com ara que ha impedit comptar amb la col·laboració de l'APDCAT en la resolució de l'incident o per determinar si la violació havia de ser comunicada a les persones afectades o no.

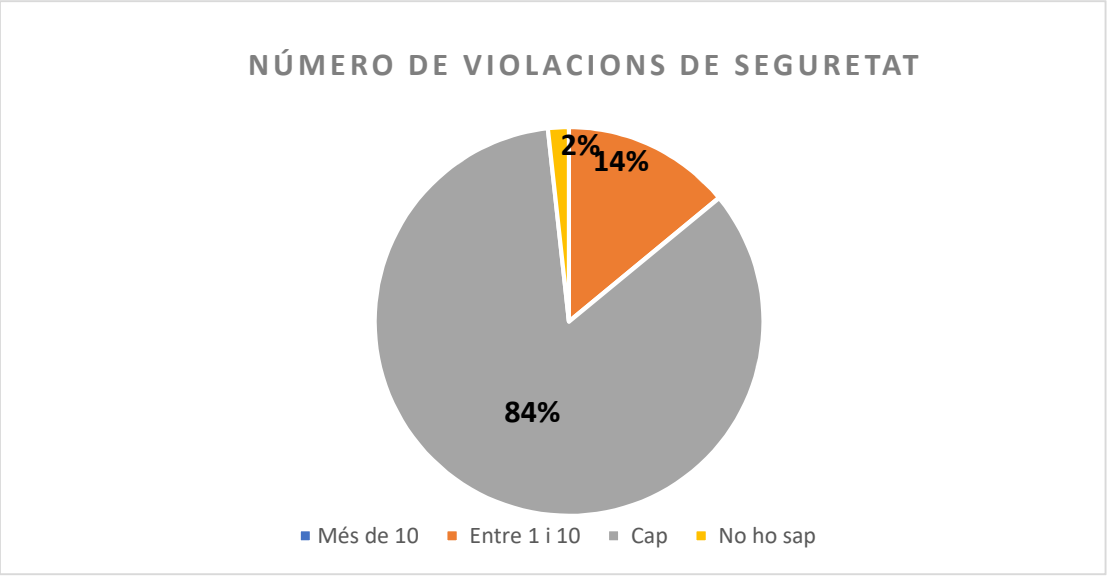


Número d'incidents o violacions de seguretat.

El responsable del tractament ha de documentar totes les violacions de seguretat, tant si és perceptiu notificar-les a l'APDCAT com si no ho és. En concret, ha de fer constar tota la informació relativa als fets, els efectes i les mesures correctores adoptades. Aquesta documentació ha d'estar a disposició de l'APDCAT (art. 33.5 RGPD).

Cap de les entitats enquestades manifesta haver sofert més de 10 violacions de seguretat. Només un 14% ha detectat entre 1 i 10 violacions de seguretat aquest últim any (setembre 2018-agost 2019).

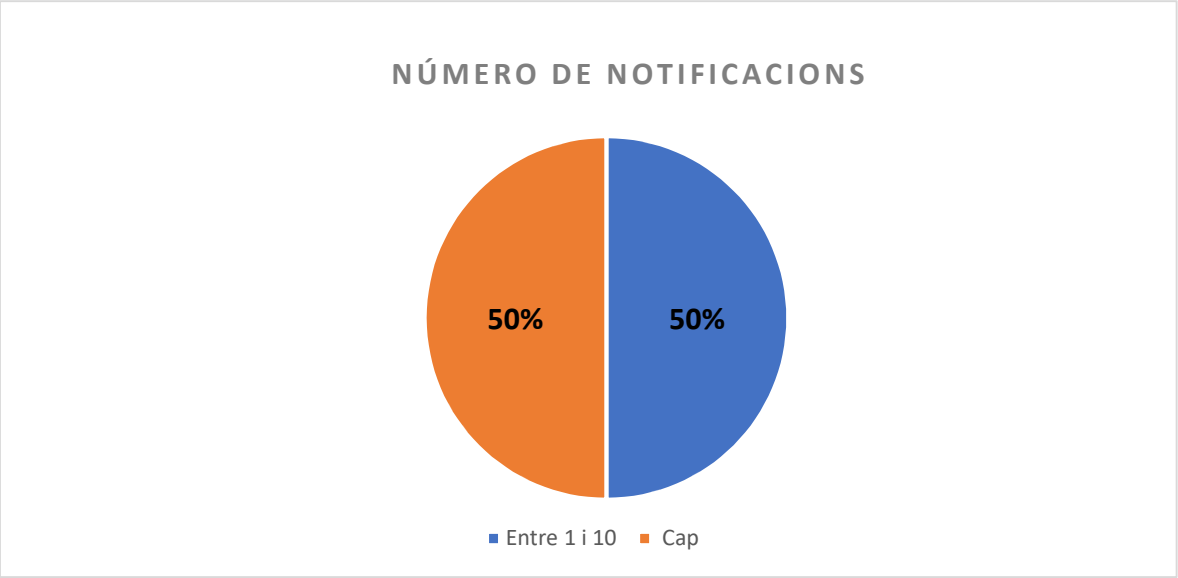
Les universitats i els departaments de l'Administració han estat els més propensos a patir incidències en les dades, circumstància que, per altra banda, pot ser fàcilment relacionada amb les dimensions d'aquestes entitats.



Número de notificacions a l'APDCAT o a altres autoritats

De les entitats que han patit violacions de seguretat, la meitat ho ha notificat a l'APDCAT. Aquesta diferència entre les violacions de seguretat sofertes i les notificades a l'APDCAT en principi podria ser atribuïble al fet que malgrat que el responsable del tractament ha de documentar totes les violacions de seguretat, no està obligat a notificar-les totes a l'autoritat.

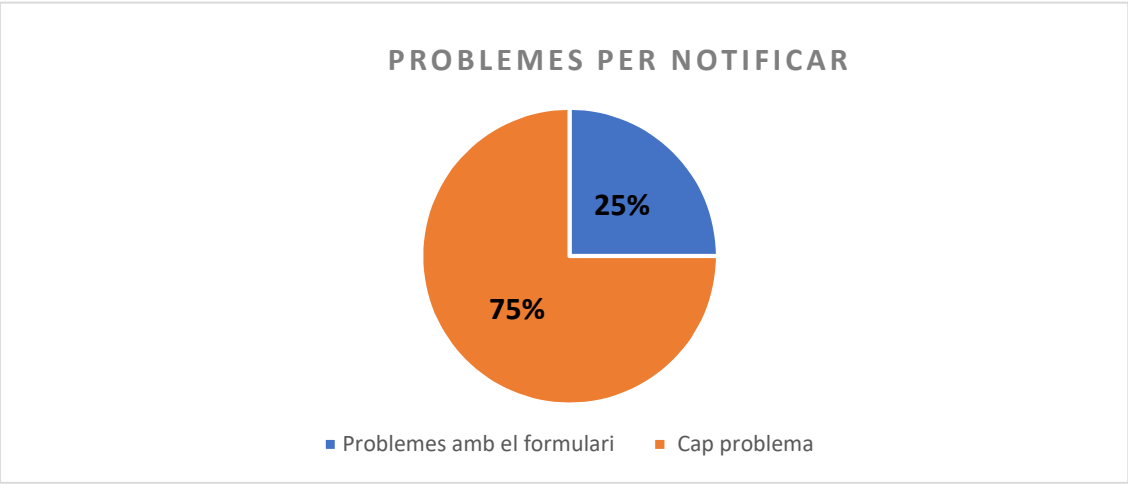
Cal tenir en compte que a més de les notificacions a l'APDCAT, altres normes sectorials, per exemple, en matèria de telecomunicacions o en matèria de ciberseguretat, també preveuen l'obligació de notificar les violacions a altres autoritats. No obstant això, cap de les entitats manifesta haver fet notificacions a altres autoritats.



Procés de notificació

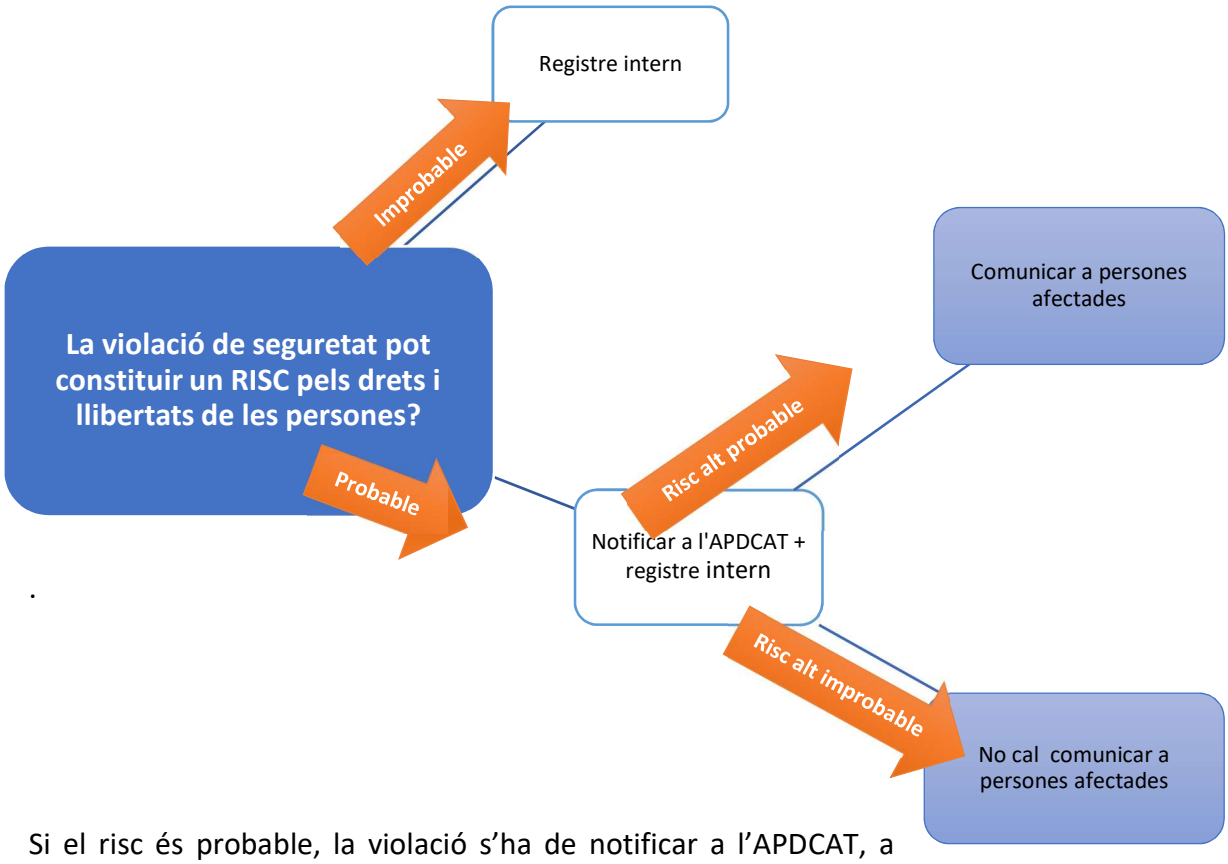
La notificació de la violació de seguretat a l'APDCAT s'ha de fer per mitjans electrònics mitjançant el formulari de notificació que es pot trobar a la seu electrònica d'aquesta Autoritat (https://apdcat.gencat.cat/ca/seu_electronica/tramits/notificacio/).

Dels casos en què s'ha dut a terme la notificació de l'incident, un 25% ha manifestat que ha tingut problemes amb el formulari. En concret han manifestat tenir dificultats per emplenar la informació requerida al formulari, atesa la limitació de temps per fer-la efectiva.



Coneixement del criteri desencadenant de la notificació

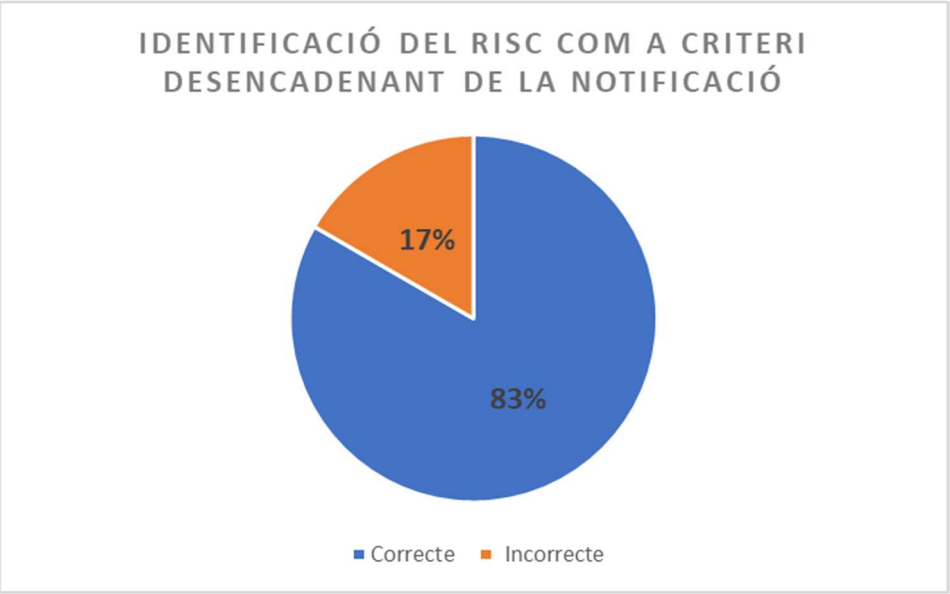
El criteri que s'ha d'utilitzar per saber si notificar o no una violació de seguretat és el criteri del risc. Només caldrà notificar aquells supòsits en què existeixi un risc pels drets i llibertats de les persones. A continuació s'adjunta un diagrama de flux sobre com els responsables del tractament han d'actuar davant una violació de seguretat amb probabilitat de constituir risc per als drets i llibertats de les persones.



.

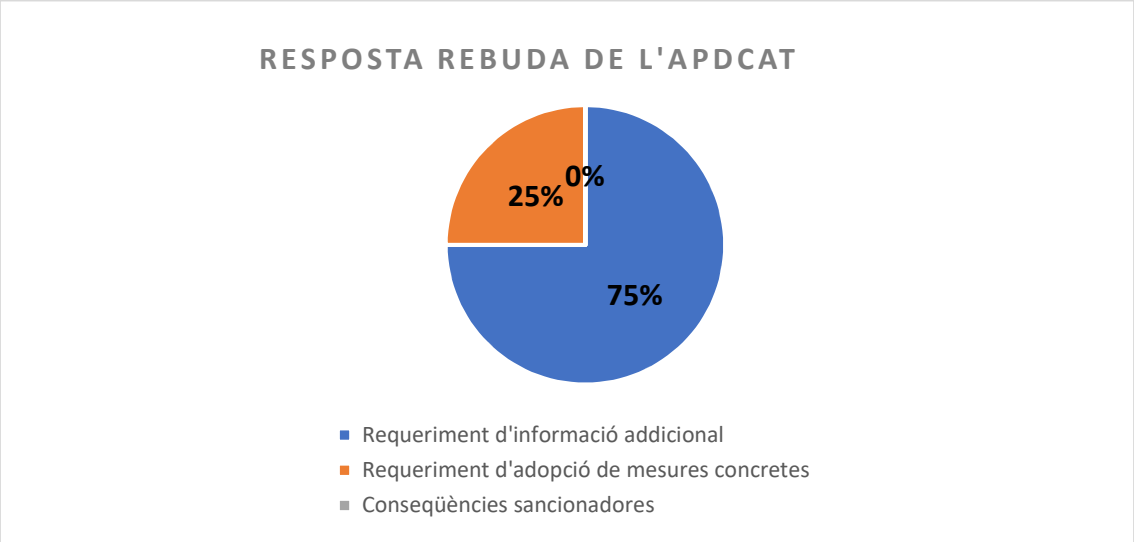
Si el risc és probable, la violació s'ha de notificar a l'APDCAT, a més de registrar-se internament. I si, a més, el risc és probablement alt, s'haurà de comunicar a les persones afectades.

En relació amb les violacions de seguretat que no han estat notificades, en l'enquesta s'ha preguntat sobre el motiu pel qual no s'han notificat. La majoria de les entitats, en concret un 83% ha sabut identificar el risc com el criteri a partir del qual s'ha de notificar un incident.



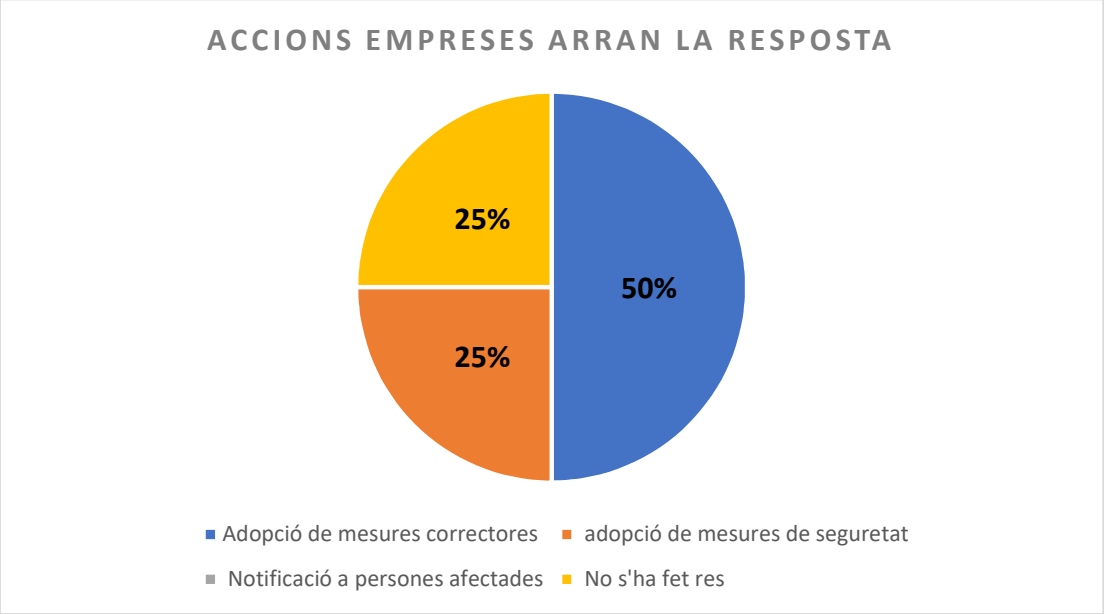
Resposta rebuda per part de l'APDCAT. Accions empreses arran la resposta. Grau de satisfacció amb la resposta rebuda.

De les entitats que han fet notificacions de violacions a l'APDCAT, el 75% manifesta que la resposta que han obtingut ha estat un requeriment d'informació addicional, mentre que el 25% restant manifesta haver rebut requeriments d'adopció de mesures concretes. Cap de les entitats enquestades ha estat sancionada pel fet de patir una violació de seguretat.

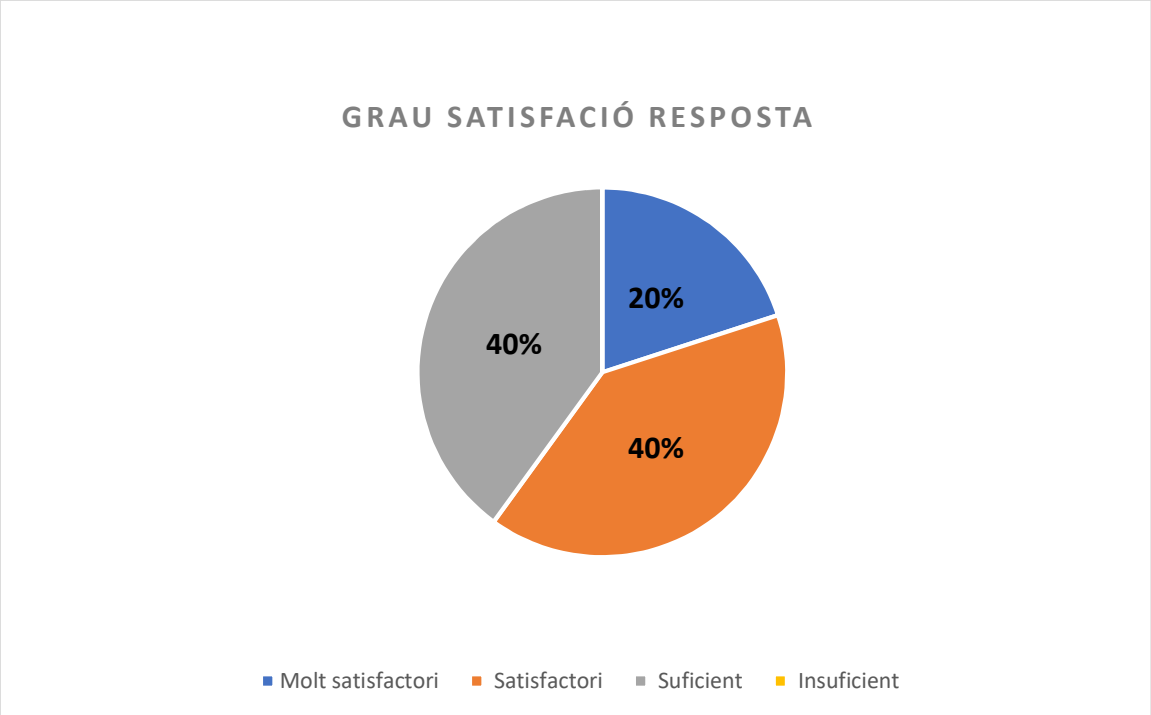


Sens perjudici que el responsable del tractament ha d'adoptar les mesures adients per donar resposta a l'incident, la resposta que es rep per part de l'APDCAT després d'haver-se produït la notificació pot ajudar a donar resposta a l'incident i a prevenir

incidents futurs. Les mesures adoptades per les entitats afectades arran la resposta de l'APDCAT han estat l'adopció de mesures correctores per posar fi a la violació (50%), adopció de mesures de seguretat addicionals (25%) mentre que en un 25% dels casos no s'han adoptat mesures addicionals a les que ja s'havien adoptat.



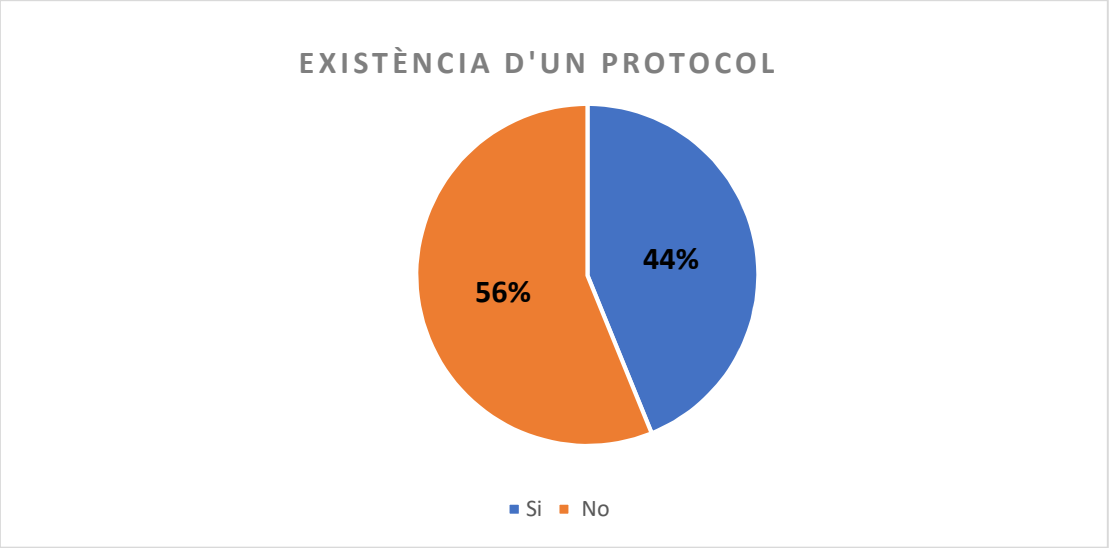
Finalment, en relació amb el grau de satisfacció per la resposta rebuda de l'APDCAT la resposta predominant és positiva, en concret, satisfactòria (40%) o molt satisfactòria (20%).



Existència d'un protocol per notificar els incidents.

Per ajudar al compliment dels articles 33 i 34 RGPD pot ser d'interès que tant el responsable com l'encarregat del tractament disposin d'un protocol per notificar els incidents, és a dir, que es documenti el procés que cal seguir un cop s'ha detectat una violació. Això inclou la manera de contenir, gestionar i recuperar-se de l'incident, així com avaluar la possible existència d'un risc o d'un alt risc i, si escau, notificar la violació a l'APDCAT i comunicar-la a les persones afectades.

De les entitats enquestades, el 44% disposa d'un protocol que ha sabut descriure breument.



De les entitats que no tenen protocol, algunes han manifestat que en el supòsit de partir un incident seguirien el diagrama de flux que mostra els requisits de notificació establert en les directrius del Grup de l'article 29 sobre la notificació de la violació de la seguretat de les dades personals segons el Reglament 2016/679.

Una breu descripció dels passos que la majoria de les entitats han establert en el protocol seria la següent:

1) Quan l'encarregat del tractament o qualsevol altre usuari detecta una violació de la seguretat es comunica de manera immediata al coordinador responsable.

2) El coordinador responsable ho comunica al delegat de protecció de dades.

3) El delegat de protecció de dades analitza el risc pels drets i llibertats de les persones físiques.

4) Si és pertinent es notifica a l'autoritat de control competent.

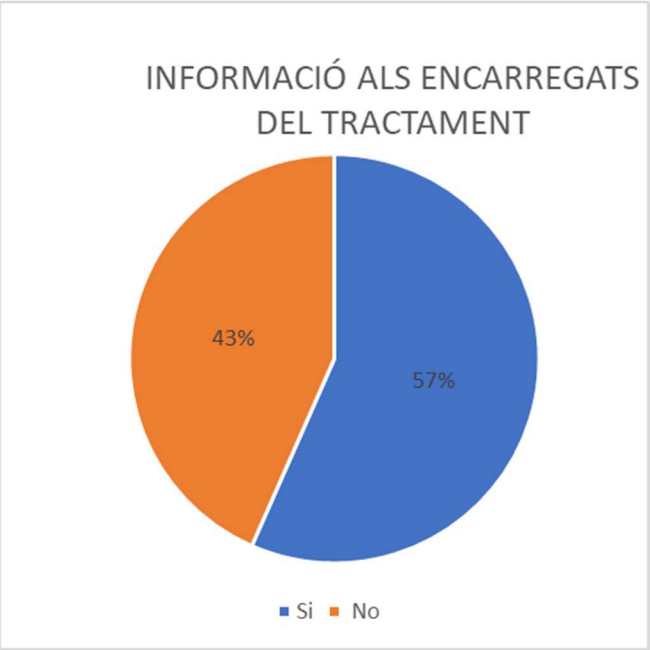
A més, el 37% de les entitats, inclouen accions per prevenir futures violacions de la seguretat.

Informació a l'encarregat del tractament.

L'article 33.2 RGPD deixa clar que si un responsable té un encarregat del tractament i aquest encarregat té constància d'una violació de la seguretat l'ha de notificar al responsable del tractament "sense dilació indeguda". De fet, l'article 28.3.f) RGPD estableix que el contracte o acte jurídic que regula l'encàrrec del tractament ha d'estipular que l'encarregat "*ha d'ajudar el responsable a garantir el compliment de les obligacions que estableixen els article 32 a 36 RGPD, tenint en compte la naturalesa del tractament i la formació a disposició de l'encarregat*".

No obstant això, el responsable és en darrer terme qui ha de garantir una resposta adequada davant un incident de seguretat.

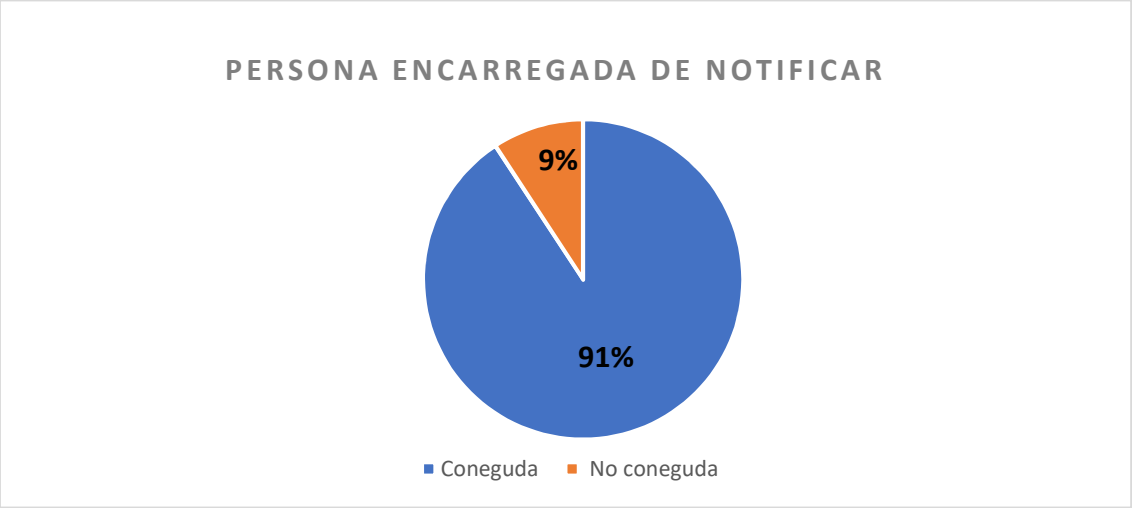
Arran la pregunta de si s'han donat instruccions als encarregats del tractament per part del responsable del tractament, sobre la forma com s'ha de gestionar un incident de seguretat, la resposta ha estat afirmativa en el 57% de les entitats, mentre que el 43 % restant manifesta que no ho ha fet.



Persona responsable de fer la notificació a l'autoritat.

Quan s'ha preguntat a les entitats enquestades si podien identificar la persona encarregada de fer les notificacions de violacions de seguretat dins de la seva organització, el 91% de les entitats han pogut identificar el càrrec de la persona a qui correspon fer la notificació. Només en cinc casos no han pogut fer-ho.

Ara bé, el càrrec encarregat de fer la notificació ha variat. La meitat han assenyalat l'òrgan específic (ja sigui el DPD o un altre), mentre que l'altra meitat només han estat capaços d'identificar el responsable, sense identificar un òrgan concret per fer aquesta tasca.



El responsable o l'encarregat del tractament pot tenir un delegat de protecció de dades, ja sigui com a requeriment de l'article 37 RGPD i l'article 34 LOPDGDD (per exemple en el cas de les administracions públiques) o voluntàriament, com a bona pràctica.

El delegat de protecció de dades ha de ser una figura clau a l'hora de prevenir o a preparar-se per fer front a una violació, proporcionant assessorament i fent el seguiment de les mesures adoptades i també en qualsevol investigació posterior que faci l'autoritat de control. En aquest sentit, en aquelles entitats que comptin amb un delegat de protecció de dades, es recomana que si es produeix una violació, el delegat de protecció de dades en sigui informat ràpidament i que intervingui en tot el procés de gestió i notificació de la violació.

II. Comunicació a les persones afectades.

Número de comunicacions a les persones afectades.

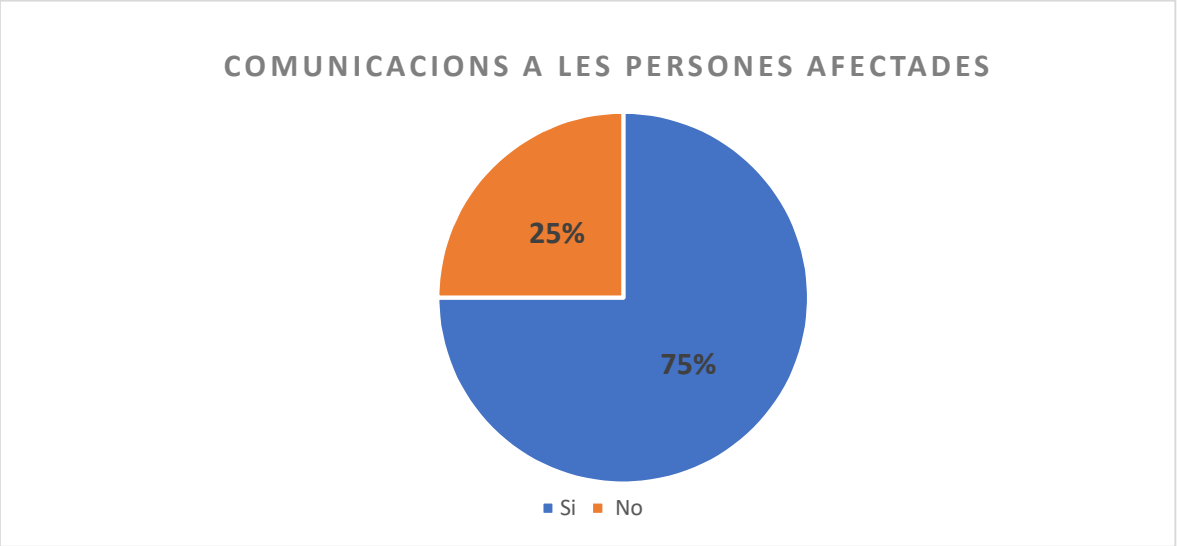
Si és probable que la violació de seguretat de les dades comporti un risc alt pels drets i llibertats de les persones físiques, el responsable l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill, tret que concorri alguna de les circumstàncies següents:

1) El responsable hagi adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades.

2) El responsable hagi aplicat mesures posteriors que garanteixen que ja no hi ha la possibilitat que es concreti el risc alt.

3) Suposi un esforç desproporcionat; en aquest cas, es pot optar per una comunicació pública o una mesura equivalent.

D'acord amb el gràfic, de les entitats que han patit alguna violació de seguretat al llarg d'aquest any (setembre 2018-agost 2019), el 75% n'ha comunicat alguna a les persones afectades. El 25% restant no n'ha comunicat cap.

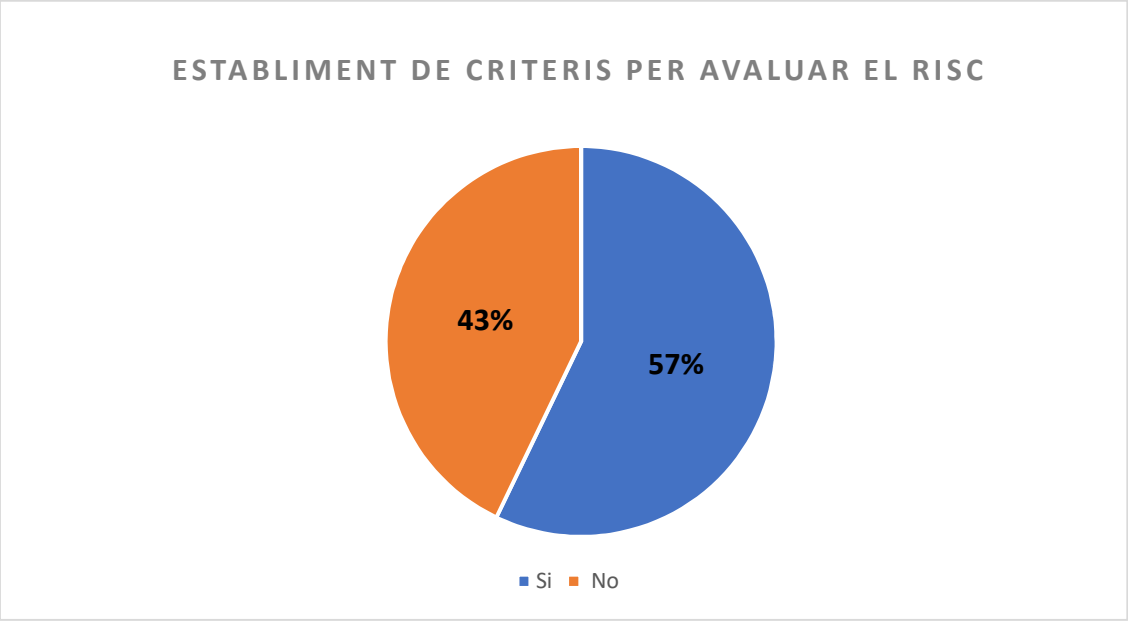


III. Identificació del risc existent

Establiment de criteris per detectar l'existència de risc.

L'element clau per determinar si cal notificar i comunicar una violació de seguretat o no és l'existència de risc, i si escau d'alt risc, per a les persones afectades.

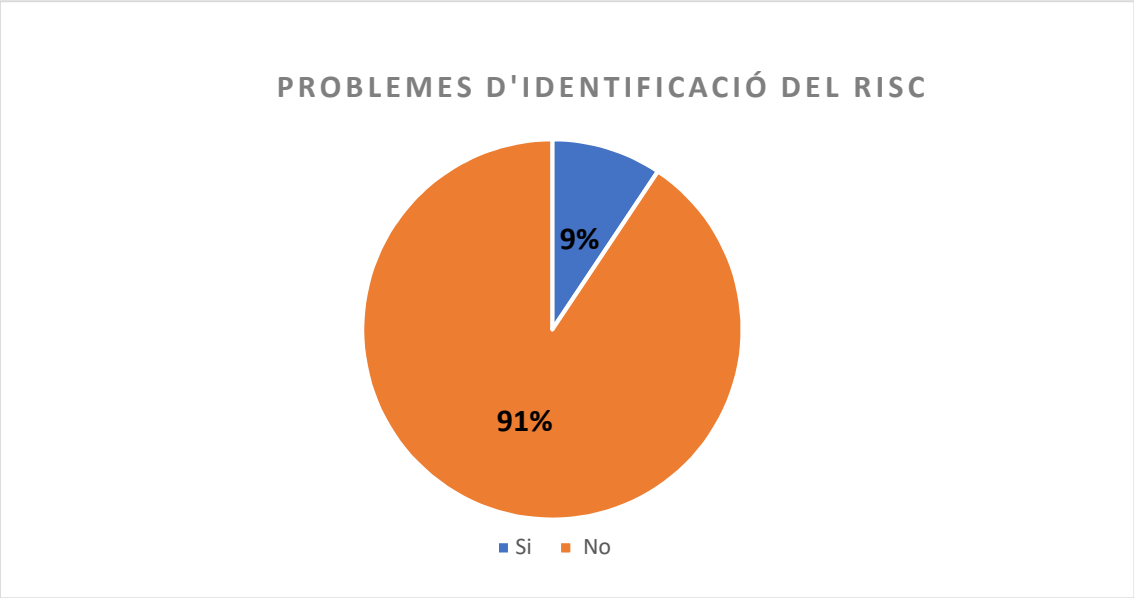
Més de la meitat de la mostra disposa de criteris aprovats per avaluar el risc. Identificar prèviament els riscos davant diferents tipus d'incidents pot ajudar a donar una resposta ràpida i acurada davant un incident de seguretat. Ara bé, cal remarcar que algunes entitats, tot i no tenir un document amb criteris establerts, manifesten seguir les recomanacions fetes per l'Agència de Seguretat de les Xarxes i de la Informació de la Unió Europea (ENISA).



Problemes per identificar el grau del risc.

A l'hora d'identificar l'existència de risc, el responsable del tractament pot tenir problemes per identificar si aquest realment existeix, i, si escau, la seva gravetat. Per això s'han de prendre en consideració les circumstàncies específiques de la violació. El Grup de Treball de l'article 29 recomana que l'avaluació tingui en compte diversos criteris com són: el tipus de violació, la naturalesa, el grau de sensibilitat i el volum de dades personals, la facilitat per identificar les persones, la gravetat de les

conseqüències pels afectats, el nombre de persones afectades, i les característiques especials tant de l'interessat com del responsable del tractament.



En el gràfic anterior es pot apreciar que només el 9% manifesta tenir problemes amb la identificació de l'existència de risc. No obstant això, existeix una clara discrepància entre la resposta a aquesta pregunta i l'obtinguda en la pregunta següent atès que, com es pot veure en les respostes donades als supòsits concrets plantejats en la pregunta següent, només un 15% de les entitats enquestades han identificat correctament si concorre o no una situació de risc en tots els quatre supòsits concrets plantejats.

Supòsits concrets de detecció del risc.

En l'enquesta s'han inclòs quatre supòsits pràctics als efectes de determinar la precisió de les entitats enquestades a l'hora de determinar si concorre o no una situació de risc pels drets i llibertats de les persones:

Supòsit 1: Pèrdua temporal d'un ordinador portàtil de la directora de l'escola que conté sense encriptar informació sobre l'historial acadèmic dels alumnes.

Sí. L'escola, com a responsable del tractament de les dades dels alumnes, té l'obligació de notificar la violació a l'Autoritat sense dilació indeguda, i en un termini màxim de 72 hores des que n'ha tingut constància, ja que pot contenir dades d'un nombre

considerable de persones, que en alguns casos poden ser sensibles, i especialment perquè es refereixen a menors d'edat.

Supòsit 2: Una persona empleada envia un correu electrònic a un usuari equivocat amb informació relativa a un expedient de serveis socials.

Si, en tot cas. Cal tenir en compte l'especial sensibilitat de la informació que pot contenir un expedient en matèria de serveis socials.

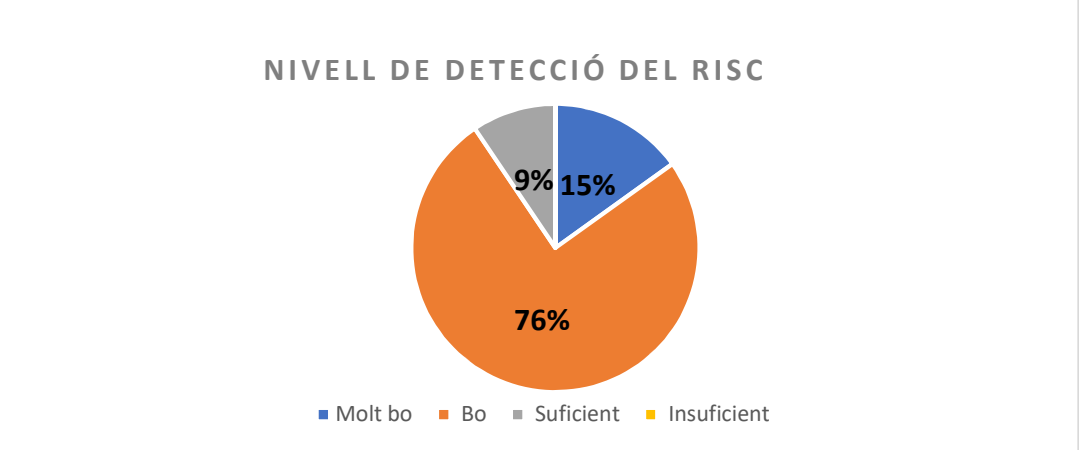
Supòsit 3: Es produeix un breu tall d'energia d'uns minuts de durada en el centre d'atenció telefònica del responsable que significa que els clients no poden trucar al responsable ni accedir als seus registres.

No. No és obligatori notificar aquesta violació, tot i que constitueix un incident de seguretat que cal registrar en virtut de l'article 33.5 RGPD.

Supòsit 4: Un hospital pateix un ciberatac a les bases de dades mèdiques que implica una falta de disponibilitat de les històries clíniques durant un període de 30 hores.

Si. L'hospital està obligat a notificar-ho com a risc alt ateses les conseqüències què per a la salut del pacient pot tenir una manca de disponibilitat, encara que sigui temporal, de la informació.

Només un 15% de les entitats enquestades ha identificat correctament el risc en els quatre supòsits. La majoria d'entitats enquestades (76%) han identificat correctament el risc en tres dels quatre supòsits; el 9% restant només ha identificat correctament dos supòsits.



CONCLUSIONS FINALS

I. Notificacions de les violacions de seguretat a l'APDCAT.

Una vegada realitzat l'anàlisi es conclou que les qüestions bàsiques, com són l'obligatorietat, el termini i les conseqüències de la gestió de les notificacions de violacions de seguretat són conegudes per la majoria d'entitats, com també del criteri del risc, com a element determinant per haver de fer o no una notificació, sense que s'apreciïn grans diferències entre els diferents tipus d'entitats que han participat a l'enquesta.

Pel que fa a les violacions de seguretat sofertes i a les notificades, destacar que les entitats amb dimensions més grans són les que han sofert un major nombre de violacions de seguretat i, conseqüentment són les que han realitzat més notificacions; també que la notificació de la violació de seguretat mitjançant el formulari disponible a la seu electrònica de l'APDCAT en algunes ocasions ha generat dificultats a causa de la limitació de temps per fer-ho.

Un cop feta la notificació s'ha constatat que la resposta més habitual ha estat el requeriment d'informació addicional, així com el requeriment d'adopció de mesures concretes. En qualsevol cas, el grau de satisfacció amb la resposta rebuda és força elevat.

Menys de la meitat d'entitats enquestades disposen d'un protocol aprovat per a la gestió de la notificació de violacions de seguretat. Totes les entitats que en disposen saben descriure'l breument i molts dels protocols inclouen accions per prevenir futures violacions de seguretat.

En general ha estat fàcil per les entitats identificar a quina persona o càrrec correspon notificar les violacions de seguretat a l'autoritat. En la majoria dels casos aquesta funció correspon al delegat de protecció de dades com a persona de contacte entre l'entitat i l'autoritat.

Finalment afegir que el número d'entitats que informen als encarregats del tractament sobre les qüestions de protecció de dades és força baix.

Comunicació a les persones afectades.

S'han produït pocs casos de violacions de seguretat amb comunicació a les persones afectes, atesa la inexistència, segons les respostes obtingudes, d'un alt risc per als drets i llibertats dels interessats.

II. Identificació del risc existent

Dels resultats obtinguts en l'enquesta es pot concloure que una mica més de la meitat d'entitats tenen aprovats criteris per determinar l'existència risc un cop produïda una violació de seguretat i poques manifesten haver tingut problemes a l'hora d'identificar la seva gravetat.

Malgrat això en relació amb els quatre supòsits concrets plantejats a l'enquesta, només un 15% ha detectat correctament la concurrència o no del risc en els quatre supòsits.

Per tot això, s'observa de forma global que existeix un bon coneixement dels requeriments en relació amb la notificació de les violacions de seguretat per part de les entitats enquestades, amb alguns punts a millorar pel que fa a la identificació del risc, la capacitat per poder recollir i transmetre dins del termini previst tota la informació que s'ha d'incloure al formulari de notificació, i també pel que fa a la informació que sobre aquesta qüestió es facilita als encarregats del tractament.

ANNEX 1. ENQUESTA

ENQUESTA *GPEN Privacy Sweep 2019*		
Data:	**Núm. resposta (*a emplenar per APDCAT*):**	
Tipus d'entitat: **Administració de la Generalitat ☐** **Universitat ☐** **Col·legi professional ☐** **Ajuntament: de ..... a ..... habitants ☐** **de ..... a ..... habitants ☐** **de menys de ..... habitants ☐**		
Mètode de contacte: **Trucada telefònica ☐** **Email ☐**		
Preguntes		
Notificació a l'APDCAT		
1.	En la vostra organització, **és obligatòria** la notificació dels incidents o violacions de seguretat a l'Autoritat Catalana de Protecció de Dades (APDCAT)? Sempre ☐ En alguns casos ☐ Mai ☐	
	En cas afirmatiu, en quin **termini?**	
	Quines poden ser les **conseqüències** de no notificar-ho?	
2.	**Quants incidents o violacions de seguretat** heu tingut a la vostra organització en el darrer any (setembre 2018-agost 2019)?	
3.	Dels incidents que heu tingut, **quants n'heu notificat** a l'APDCAT en el darrer any (setembre 2018-agost 2019)?	
	Alguns d'aquests incidents l'heu notificat a **alguna *altra autoritat***? Sí ☐ No ☐	
	En cas afirmatiu, a **quina?**	
4.	Heu tingut algun **problema** per poder fer la notificació? Sí ☐ No ☐	

	En cas afirmatiu**, quins**?
5.	Si no heu notificat alguna violació de seguretat, quin ha estat el **motiu**?
6.	Quina **resposta** heu rebut arran la notificació?
	Quines **accions** heu hagut d'emprendre arran la notificació?
	Quin és el **grau de satisfacció** amb la resposta rebuda? Molt satisfactori ☐ Satisfactori ☐ Suficient ☐ Insuficient ☐
7.	Teniu aprovat un **protocol** per notificar els incidents o violacions de seguretat? Sí ☐ No ☐
	Podeu descriure'l breument?
	Aquest inclou accions per prevenir futures violacions de la seguretat? Sí ☐ No ☐
	A qui (**càrrec**) correspon la notificació de les violacions de seguretat en la vostra organització?
	Heu donat instruccions als vostres **encarregats del tractament** sobre aquesta qüestió? Sí ☐ No ☐
Comunicació a les persones afectades	
8.	Quantes comunicacions de violacions de seguretat heu fet a les **persones afectades**?

Identificació del risc existent	
9.	Teniu aprovat algun tipus de criteri per avaluar el risc quan s'ha produït una violació de seguretat? Sí ☐ No ☐
	Heu tingut **problemes per identificar** els supòsits en que sí que era obligatori notificar les violacions de seguretat? Sí ☐ No ☐
	Quins han estat els supòsits més **problemàtics**?
10.	Podríeu establir si seria obligatòria la notificació a l'APDCAT en els **supòsits següents**?
	Supòsit 1: Pèrdua temporal d'un ordinador portàtil de la directora de l'escola que conté sense encriptar informació sobre l'historial acadèmic dels alumnes Obligatòria ☐ No obligatòria ☐ Depèn de les circumstàncies ☐
	Supòsit 2: Una persona empleada envia un correu electrònic a un usuari equivocat amb informació relativa a un expedient de serveis socials Obligatòria ☐ No obligatòria ☐ Depèn de les circumstàncies ☐
	Supòsit 3: Es produeix un breu tall d'energia d'uns minuts de durada en el centre d'atenció telefònica del responsable que significa que els clients no poden trucar al responsable ni accedir als seus registres Obligatòria ☐ No obligatòria ☐ Depèn de les circumstàncies ☐
	Supòsit 4: Un hospital pateix un ciberatac a les bases de dades mèdiques que implica una falta de disponibilitat de les històries clíniques durant un període de 30 hores.

	Obligatòria ☐ No obligatòria ☐ Depèn de les circumstàncies ☐