**PÍNDOLA 23.- CRITERIS PER L'ANÀLISI DE NVS**

La Guia per la gestió i notificació de violacions de seguretat publicada per la Agència Espanyola de Protecció de Dades (AEPD) està orientada a proporcionar directrius generals en la gestió d'incidents i, especialment, a aquells casos en els quals l'incident tingui o pugui tenir incidència en l'àmbit del RGPD[1], és a dir, en aquells casos en els quals l'incident de seguretat pugui afectar els drets i llibertats de les persones. D'altra banda, cal tenir en compte que en l'àmbit del RGPD la notificació podria no realitzar-se quan sigui improbable que l'incident de seguretat constitueixi un risc per als drets i llibertats de les persones físiques.

De manera orientativa es proposa en l'Annex III de la guia, un model que pot ser utilitzat com a referència en la presa de decisions tant per a la notificació a l'Autoritat de Control com als propis interessats. En cada cas s'ha de valorar els llindars sota els quals el responsable procedirà a la notificació.

A continuació us detallem en els següents apartats d'aquesta píndola les pautes per dur a terme l'anàlisi:

1. Procediment d'anàlisi d'una probable violació de seguretat
2. Fórmula de càlcul de gravetat d'un incident de seguretat que afecti a dades personals i presa de decisions per notificació al CPD per part de les unitats que hagin detectat l'incident (sistemes, atenció ciutadà,...)
3. Interpretació de resultats[2]
4. Criteris de classificació
5. Exemples d'incident - Classificació i anàlisi de l'incident.

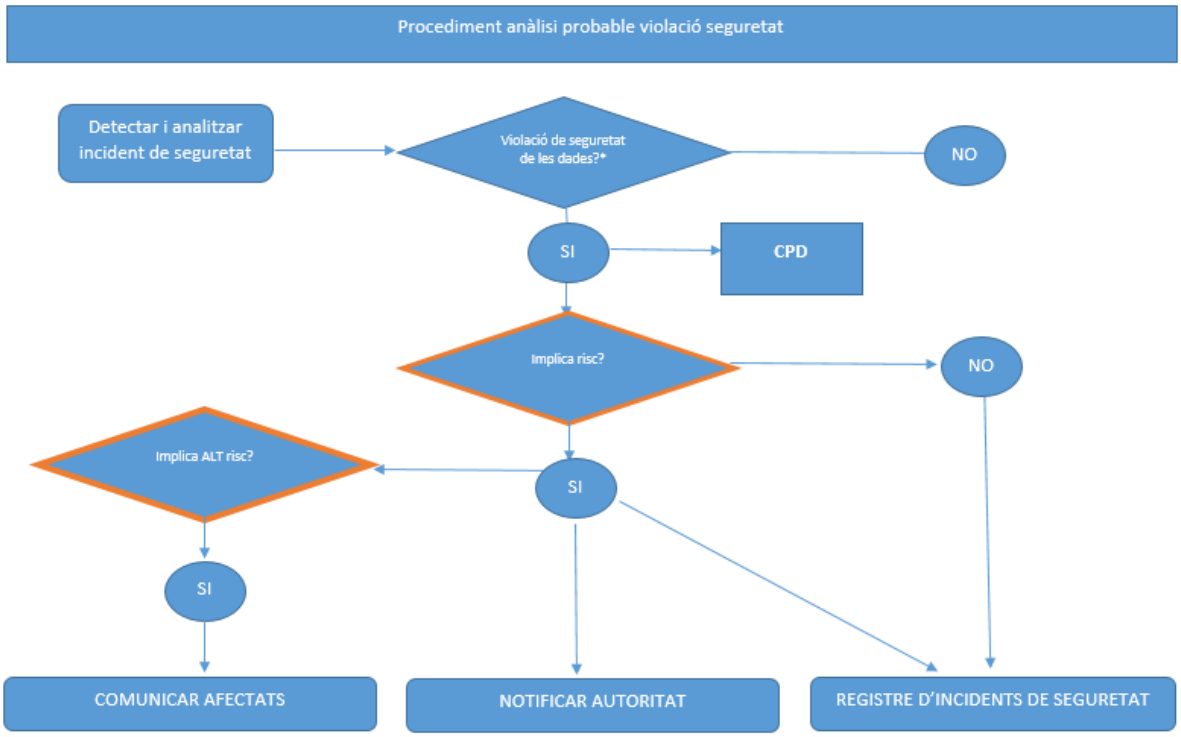
**-Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut-**

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.)

[1] Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.

[2] Criteri "*Guía para la gestión y notificación de brechas de seguridad Agència Española de Protección de datos*".

## 1. PROCEDIMENT ANÀLISI PROBABLE VIOLACIÓ DE SEGURETAT



## 2. CÀLCUL GRAVETAT D'UN INCIDENT DE SEGURETAT QUE AFECTI A DADES PERSONALS I PRESA DE DECISIONS PER NOTIFICACIÓ A CPD

### A. Càlcul en base a 3 paràmetres (volum, tipologia i impacte):

**1) VOLUM** (número de registres complerts e identificats)

- Menys de 100 registres (1)
- Més 1.000 (2)
- Entre 1.000 i 100.000 (3)
- **Més de 100.000 (4)**
- **Més de 1.000.000 (5)**

**2) TIPOLOGIA DE DADES** (Segons RGPD)

- Dades no sensibles (x1)
- **Dades sensibles (x2)**

**3) IMPACTE** (EXPOSICIÓ)

- Nul (2)
- Intern (dintre de l'empresa - controlat) - (4)
- **Extern (Perímetre proveïdor, atacant) - (6)**
- **Públic (Accessible a Internet) - (8)**
- **Desconegut (10)**

### B. Fórmula de càlcul:

**Risc** = P x I

**Risc** = P (Volum) x Impacte (Tipologia x Impacte)

## 3. INTERPRETACIÓ RESULTATS

- Es recomana notificar violació de seguretat a APDCAT si:
    - Risc amb valor quantitatiu superior a 20
    - Si coincideixen dos de les circumstàncies marcades en **vermell** als paràmetres del càlcul.

- Es recomana comunicar als afectats si:
    - Risc amb valor quantitatiu superior a 40
    - Si coincideixen dos de les circumstàncies marcades en **vermell** als paràmetres del càlcul.

## 4. CRITERIS DE CLASSIFICACIÓ

| | |
|---|---|
| **Tipus d'incident** | **Incident de confidencialitat:** té lloc quan parts no autoritzades, o sense propòsit legítim per accedir a la informació, accedeixen a ella. La gravetat de la pèrdua de confidencialitat s'haurà de veure juntament amb l'abast de la seva divulgació, és a dir, número potencial i tipus de parts que poden haver accedit a la informació. |
| | **Incident d'integritat:** té lloc quan hi ha alteració de la informació original i la substitució de dades pot ser perjudicial per l'individu. La situació més greu ocorre quan existeixen possibilitat de que les dades alterades s'hagin utilitzat d'una manera que pugui fer mal a l'individu. |
| | **Incident de disponibilitat:** té lloc quan no es pot accedir a les dades originals quan és necessari. Pot ser temporal (dades recuperables) o permanent (dades no recuperables). |
| **Taxonomia** | **Vulnerabilitat no coneguda:** vulnerabilitat que permet a un atacant l'accés a dades en la mesura en que és una vulnerabilitat desconeguda. Serà necessari que el fabricant o desenvolupador la resolgui. |
| | **Atac dirigit:** s'establirien en aquest tipus d'incident, per exemple campanyes amb enviament de mails amb software maliciós a treballadors de l'entitat fins a aconseguir que algú ho instal·li a l'equip o sigui porta d'entrada al sistema. |
| | **Denegació de servei:** ofegar de tràfic al sistema fins que no sigui capaç de donar servei als usuaris legítims del mateix. |
| | **Accés a comptes privilegiades:** l'atacant accedeix al sistema mitjançant un usuari administrador. En aquest cas, prèviament, deu haver aconseguit l'usuari i contrasenya per algun altre mitjà. |
| | **Codi maliciós:** pot ser que un usuari ho instal·li de manera involuntària. |
| | **Compromís de la informació:** incidents relacionats amb accés i fuita, modificació o esborrament d'informació no pública. |
| | **Robatori, pèrdua i/o filtració de dades:** inclou dispositius amb informació. |
| | **Desfiguració:** Atac dirigit que modifica la pàgina web corporativa. |
| | **Vulnerabilitat del sistema:** un possible atacant aconsegueix explotar amb èxit una vulnerabilitat existent al sistema o comprometre una aplicació de l'entitat. |
| | **Engany/spam:** s'indueix a l'usuari a clicar sobre un enllaç pensant que es correcte. |
| **Tipologia de dades** | **Dades no sensibles:** enteses com les dades de contacte, educació, familiars, professionals, econòmiques |
| | **Dades sensibles**: salut, biomètriques, vida sexual, religió |
| **Origen de l'incident** | **Font interna**: organització |
| | **Font externa:** proveïdors de serveis, ciutadà, encarregat de tractament) |
| **Gravetat** | **Crític**: afecta a dades valuoses o gran volum i poc temps. |

| | |
|---|---|
| | **Molt Alt:** volum apreciable i pot afectar a dades valuoses. |
| | **Alt:** pot afectar a dades valuoses |
| | **Mitjana**: afecta a un volum apreciable |
| | **Baix:** escassa o nul·la capacitat a d'afectar a dades valuoses o volum apreciable. |
| **Volum** | Menys de 100 registres |
| | Més 1.000 |
| | Entre 1.000 i 100.000 |
| | Més de 100.000 |
| | Més de 1.000.000 |

## 5. EXEMPLES D'INCIDENT - CLASSIFICACIÓ I ANÀLISI

**EXEMPLE 1**

**CLASSIFICACIÓ**

Consulta dels criteris de classificació apartat 4.

| | |
|---|---|
| **Tipus d'incident** | Confidencialitat |
| **Taxonomia** | Accés a conta privilegiada |
| **Tipologia de dades** | Dades sensibles |
| **Origen de l'incident** | Extern |
| **Gravetat** | Alta |
| **Volum aproximat** | Menys de 100 registres |

**ANÀLISI**

| | | |
|---|---|---|
| **Volum** | Menys de 100 registres | 1 |
| **Tipologia de dades** | Dades sensibles | 2 |
| **Impacte** | Alta | 8 |
| **Risc** | **1 x (8x2)** | **16** |

**INTERPRETACIÓ:**

- Es recomana notificar violació de seguretat a APDCAT, ja que coincideixen dos de les circumstàncies marcades en **vermell** als paràmetres del càlcul

- Es recomana comunicar als afectats, ja que coincideixen dos de les circumstàncies marcades en **vermell** als paràmetres del càlcul

**EXEMPLE 2**

**CLASSIFICACIÓ**

Consulta dels criteris de classificació apartat 4.

| | |
|---|---|
| **Tipus d'incident** | Confidencialitat |
| **Taxonomia** | Compromís de la informació |
| **Tipologia de dades** | Dades sensibles |
| **Origen de l'incident** | Extern |
| **Gravetat** | Alta |
| **Volum aproximat** | Més de 200.000 registres |

**ANÀLISI**

| | | |
|---|---|---|
| **Volum** | Mes de 200.000 registres | 4 |
| **Tipologia de dades** | Dades sensibles | 2 |
| **Impacte** | Alta | 8 |
| **Risc** | **4 x (8x2)** | **64** |

**INTERPRETACIÓ**

- Es recomana notificar violació de seguretat a APDCAT Risc amb valor quantitatiu superior a 20

- Es recomana comunicar als afectats Risc amb valor quantitatiu superior a 40