Píndola 52.- Resum de la Guia 01/2021 - Exemples de Notificacions de Violacions de Seguretat (NVS), del Comitè Europeu de Protecció de Dades

(Versió 2.0)

El Comitè Europeu de Protecció de Dades[1] (EDPB) ha publicat la Guia 01/2021 *on Examples regarding Data Breach Notification*[2], on s'exemplifiquen diferents **escenaris de violacions de seguretat** amb l'objectiu d'ajudar als responsables del tractament a **notificar les violacions** de seguretat, **gestionar-les** i determinar quins factors cal tenir en compte durant **l'avaluació de l'impacte** produït.

I. Introducció

L'RGPD[3] introdueix l'obligació de notificar una violació de dades personals a l'autoritat competent, en el nostre cas l'APDCAT, així com a la persona afectada (Art. 33 i 34). Donat que l'anterior directiu no aborda totes les qüestions pràctiques amb suficient detall, sorgeix la necessitat de realitzar una guia específica. Aquest document pretén complementar, en cap cas substituir, les **directrius del grup de treball sobre protecció de dades de l'article 29**[4] i reflexa les experiències comunes de les autoritats nacionals competents. El seu objectiu es ajudar als responsables del tractament a decidir com gestionar les violacions de dades i quins factors s'han de tenir en compte durant l'avaluació de riscos.

Segons la Taula Europea de Proteccions de Dades les infraccions es poden classificar d'acord amb els següents principis coneguts:

- **Violació de la Confidencialitat**: Divulgació no autoritzada o accidental de les dades personals.
- **Violació de la Integritat**: Alteració no autoritzada o accidental de les dades personals.
- **Violació de la Disponibilitat**: Pèrdua no autoritzada o accidental de les dades personals.

Segons l'RGPD, un violació de seguretat inclou la pèrdua del control sobre les dades personals, la limitació dels drets, la discriminació, la usurpació d'identitat o frau, la reidentificació no autoritzada de la pseudonimització, el dany a la reputació i la pèrdua de confidencialitat en les dades personals protegides sota secret professional. També pot incloure qualsevol adversitat econòmica o social significativa.

Qualsevol modificació de les circumstancies dels casos que es descriuen a continuació es poden donar a diferents nivells de risc pel que es requereix mesures diferents o addicionals. Aquestes directrius estructuren els casos segons determinades categories de violacions i en cada cas s'exigeixen determinades mesures per a la mitigació que no necessàriament es repeteixen a la mateixa categoria. La documentació interna d'una infracció és una obligació independent dels riscos corresponents i han de realitzar-se en tots els casos.

[1] https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_es
[2] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_es
[3] https://www.boe.es/doue/2016/119/L00001-00088.pdf
[4] https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf

II. Ransomware

Una causa freqüent de notificació de violació de dades és un atac *ransomware* patit pel responsable del tractament, el qual es pot identificar com a violació de disponibilitat. En aquest casos s'encripten les dades personals i/o dispositius i posteriorment es demana un rescat.

La probabilitat de que un atac *ransomware* tingui èxit es pot reduir dràsticament reforçant la seguretat del entorn de control de dades. La gran majoria d'aquestes filtracions es poden evitar assegurant-se que s'han pres mesures de seguretat organitzatives, físiques i tecnològiques. Trobem exemples d'aquestes mesures en la gestió adequada de sistemes actualitzats i l'ús d'un sistema de detecció antimalware apropiat i actualitzat, així com disposar d'una copia de seguretat adequada i separada, la qual fa mitigar les conseqüències d'un atac. A més a més, un **programa de formació, educació i conscienciació** en matèria de seguretat ajudarà a prevenir i reconèixer aquests tipus d'atacs.

Per avaluar aquests riscos, el responsable del tractament ha d**'investigar la bretxa i identificar el tipus de codi maliciós per comprendre les possibles conseqüències del atac**, a més de considerar el risc per a les persones degut a la violació.

Sense **una copia de seguretat**, el responsable del tractament pot adoptar poques mesures per sanar la pèrdua de dades. L'oportunitat d'una **restauració efectiva** de les dades a partir de la copia de seguretat és una variable clau. El RGPD estableix que una violació de dades personals ha de ser notificada sense demora i amb un termini màxim de **72 hores.**

III. Atacs de Filtració d'Informació

Els atacs que aprofiten vulnerabilitats dels serveis oferts a tercers a través d'Internet es poden semblar als atacs *ransomware* en el sentit en que el risc emana de l'acció d'un tercer no autoritzat, però aquests atacs solen tenir com a objectiu copiar, filtrar i abusar de les dades personals amb una finalitat maliciosa. Per tant, son principalment violacions de la confidencialitat i de la integritat de les dades. Al mateix temps, si el responsable del tractament és conscient de les característiques d'aquests tipus d'atacs, existeixen moltes mesures a disposició dels responsables del tractament que poden reduir considerablement el risc.

La seguretat del entorn del responsable del tractament és extremadament important, ja que la majoria d'aquestes violacions poden evitar-se assegurant que tots els sistemes s'actualitzin constantment, que les dades sensibles estiguin xifrades i que les aplicacions es desenvolupin d'acord amb els estàndards de seguretat com autenticació forta i mesures contra atacs de força bruta o especialitzats. També es requereixen auditories periòdiques de seguretat informàtica, avaluacions de vulnerabilitats i proves de *pentesting* per a detectar per avançat aquests tipus de riscos i posar-hi solució.

Per a que aquesta **mitigació sigui ràpida i eficaç**, el responsable del tractament ha de tenir un **pla de resposta a incidents** que especifiqui les mesures necessàries a prendre. La naturalesa, la sensibilitat i el volum de les dades personal afectades en la violació han d'avaluar-se per a determinar fins a quin punt la violació ha afectat a les persones interessades.

Si es possible, després de solucionar el problema, la base de dades ha de comparar-se amb l'emmagatzemada en la còpia de seguretat. El responsable del tractament ha de solucionar els sistemes informàtics afectats, posar fi a la vulnerabilitat i aplicar noves mesures de seguretat per impedir accions similars en un futur. Si les dades no només s'han filtrat sinó que també s'han eliminat, el responsable del tractament ha de prendre mesures sistemàtiques per recuperar-les en l'estat en que es trobaven abans de la violació. Això podria requerir que es tingues un sistema dissenyat per a retenir arxius d'entrada diaris en cas que necessitin ser processats de nou i un mètode robust d'emmagatzemament així com una **política de retenció adequada**.

Per tot això, com es probable que aquesta violació suposi un alt risc per als drets i llibertats de les persones, **els interessats han de ser informats d'acord amb l'article 34.1 del RGPD**.

A continuació s'enumeren una sèrie de mesures recomanables per poder mitigar els riscos:

- **Xifrat i gestió de claus** d'última generació i l'ús de mètodes d'autenticació que evitin la necessitat de processar les contrasenyes a la banda del servidor és preferible així com la utilització de tallafocs
- Mantenir el **sistema actualitzat**. El responsable del tractament ha de mantenir un registre de totes les actualitzacions realitzades incloent també el moment en què es van aplicar.
- Normes de **desenvolupament segur**.
- **Política de gestió sòlida** de privilegis d'usuari i control d'accés.
- **Auditories sistemàtiques de seguretat** informàtica i avaluacions de vulnerabilitat.
- **Revisions i proves periòdiques** per garantir que les còpies de seguretat es puguin utilitzar per restaurar qualsevol dada la integritat o disponibilitat de les quals s'hagi vist afectada.
- No utilitzar ID de sessió a la URL en text pla.

IV. Factor Humà

S'ha de tenir en compte el paper del factor en les violacions de les dades personals. Donat que aquests tipus de violacions poden ser **no intencionades tant com intencionades**, és molt difícil per als responsables del tractament identificar les vulnerabilitats i adoptar mesures per evitar-les. No existeix una solució única per aquests tipus de casos, però una mirada sistemàtica pot ajudar a prevenir-los. Cal dir que la **gran majoria de violacions de dades personals venen precedides per un error de factor humà dins de la mateixa organització.**

La resolució del Comissionat de Protecció de Dades i Privacitat diu que s'han d'adoptar **mesures de salvaguarda adequades** per evitar errors de caràcter humà i proporciona una llista no exhaustives d'aquestes:

- Implementació periòdica de **programes de formació, educació i conscienciació** dels empleats sobre les seves obligacions en matèria de privadesa i seguretat, així com sobre la detecció i notificació d'amenaces a la seguretat de les dades personals.
- **Establiment de pràctiques, procediments i sistemes** de protecció de dades i privadesa sòlids i eficaços.
- Elaboració de **polítiques de control d'accés adequades** i obligar els usuaris a seguir les normes.
- Aplicar **tècniques per forçar l'autenticació** de l'usuari quan accedeixi a dades personals sensibles.
- **Desactivar el compte** de l'usuari relacionat amb l'empresa tan bon punt la persona deixi l'empresa.

- Comprovar el flux de dades inusual entre el servidor de fitxers i les estacions de treball dels empleats.
- Revisar la **política d'accés** dels empleats.
- **Desactivar els serveis oberts al núvol**.
- **Prohibir i impedir l'accés a serveis de correu oberts coneguts**.
- **Desactivar la funció d'impressió de pantalla al sistema operatiu**.
- Aplicar una **política d'escriptori net**.
- Bloqueig automàtic de tots els ordinadors després d'un temps d'inactivitat.
- Utilitzar mecanismes per canviar ràpidament d'usuari en entorns compartits.
- Ús de **sistemes dedicats a la gestió de dades personals** que apliquin mecanismes adequats de control d'accés i que evitin els errors humans.

V. Pèrdua o Robatori de Dispositius i Documents

Un tipus freqüent de violació de seguretat és la pèrdua o robatori de dispositius amb documents confidencials o dades sensibles. En aquests casos, el responsable del tractament ha de tenir en compte les circumstancies de l'operació, així com el tractament de les dades emmagatzemades en el dispositiu, el dispositiu en sí, els actius de backup i les mesures adoptades abans de la violació per a assegurar un nivell de seguretat adequat. Aquests tipus de violacions es poden classificar com a violacions de confidencialitat, però també es podria considerar violacions de disponibilitat i integritat en el cas que no existeixi una copia de seguretat.

En el moment de tenir constància de la violació, el responsable del tractament ha d'avaluar la font de risc, els sistemes, el tipus de dada i les possibles implicacions d'aquesta violació. A continuació es fa esmena d'algunes mesures recomanables:

- Activar el **xifratge** del dispositiu.
- Utilitzar un **codi d'accés/contrasenya** a tots els dispositius.
- Utilitzar **l'autenticació multifactorial**.
- **Activar les funcionalitats dels dispositius** altament mòbils que permetin la seva localització en cas de pèrdua o pèrdua.
- Utilitzar MDM (**Mobile Device Management**) amb la funció d'esborrament remot i localització. Utilitzar filtres anti-glare. Tanqueu els dispositius desatesos.
- Si és possible i adequat per al tractament de dades en qüestió, desar les dades personals no en un dispositiu mòbil sinó en un servidor central.
- Si el lloc de treball està connectat a la LAN corporativa, fer una **còpia de seguretat automàtica** de les carpetes de treball sempre que sigui inevitable que les dades personals s'emmagatzemin allà.
- Utilitzeu una **VPN** segura per connectar els dispositius mòbils als servidors de back-end.
- Proporcioneu **panys físics** als empleats perquè puguin assegurar físicament els dispositius mòbils que utilitzen mentre romanen desatesos.
- **Regulació adequada de l'ús** dels dispositius dins i fora de l'empresa.
- Utilitzar una **gestió centralitzada dels dispositius** amb un mínim de drets perquè els usuaris finals puguin instal·lar el programari.
- Instal·leu **controls d'accés físic**.
- **Eviteu emmagatzemar informació sensible** als dispositius mòbils o als discos durs.
- Si cal accedir al sistema intern de l'empresa, cal utilitzar **canals segurs** com els indicats anteriorment.

VI. Enginyeria Social

En el cas que mitjançant enginyeria social aconsegueixin prendre de manera il·lícita la identitat d'una persona i tenint en compte que aquest tipus de violació presenta un alt nivell de risc, ja que qualsevol dada sobre la persona afectada podria donar informació sobre la vida privada i podria provocar danys materials o prendre possessió de comptes, la **mesura d'autenticació adequada ha de complir un grau elevat**, en funció de les **dades personals que puguin tractar-se**. En conseqüència és necessari que el responsable realitzi tant una notificació a l'APDCAT com a la persona afectada. A més a més l'organització ha d'utilitzar una forma d'autenticació que doni lloc a un alt grau de confiança on es pugui confirmar que l'usuari identificat sigui la persona prevista. Una solució possible a això seria la utilització **d'un mètode d'autenticació multifactorial.**

En el cas que algun tipus d'informació es filtri, les dades podrien ser utilitzades per facilitar altres atacs, com la suplantació d'identitat, pel que la violació d'aquestes dades resulta un greu risc per als drets i llibertats de les persones. Aquesta violació ha de ser comunicada a tots els empleats de l'organització. Després de tenir coneixement de la filtració el responsable del tractament ha de introduir certes mesures mitigadores, com el canvi de contrasenyes. A més de notificar al proveïdor de serveis de correus i xarxa sobre l'atac. Com alternativa, també podria eliminar el dret dels usuaris a establir regles de reenviament.

Aquesta mena d'atacs han de ser abordats sense demora i centrar-se sobretot en les revisions d'automatització i controls de canvi, deteccions d'incidents i mesures de resposta.

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:
dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/dpd-salut/
Tel.: 93 553 26 42 (9:00 a 14:00 h.)