Comitè Europeu de Protecció de Dades (CEPD)

Directrius 1/2021

sobre exemples de notificació de violacions de seguretat de les dades personals

Adoptades el 14 de desembre de 2021

Versió 2.0

(Traducció no oficial al català del text oficial publicat en anglès, revisat amb l'espanyol)
Guidelines 1/2021 on Examples regarding Personal Data Breach Notification (version 2.0)
Directrices 1/2021 sobre ejemplos de notificación de violacions de la seguridad de los datos personales (versión 2.0)

Historial de versions

Versió 1.0	14/01/2021	Adopció de les Directrius per a exposició pública
Versió 2.0	14/12/2021	Adopció de les Directrius després de l'exposició pública

Índex

El Comitè Europeu de Protecció de Dades

Vist l'article 70.1.*e* del Reglament (UE) 2016/679 del Parlament Europeu 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 i pel qual es deroga la Directiva 95/46/CE (RGPD),

Vist l'Acord sobre l'Espai Econòmic Europeu i, en particular, l'annex XI i el Protocol 37, modificat per la Decisió del Comitè conjunt de l'EEE núm. 154/2018, de 6 de juliol de 2018,[1]

Vistos els articles 12 i 22 del seu Reglament intern,

Vista la comunicació de la Comissió al Parlament Europeu i al Consell titulada "La protecció de dades com a pilar de l'empoderament de la ciutadania i de l'enfocament de la UE per a la transició digital: dos anys d'aplicació del Reglament general de protecció de dades",[2]

Ha adoptat les directrius següents

1 INTRODUCCIÓ

1. En determinats casos, l'RGPD introdueix l'obligació de notificar una violació de la seguretat de les dades personals a l'autoritat nacional de control competent (AC) i comunicar-la a les persones físiques titulars de les dades que s'han vist afectades per la violació (articles 33 i 34).

2. L'octubre de 2017, el Grup de treball de l'article 29 ja va presentar una orientació *general* sobre la notificació de violació de la seguretat de les dades, en què analitzava les seccions pertinents de l'RGPD (Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el Reglament 2016/679, WP 250)[3] (d'ara endavant, Directrius WP250). Tanmateix, per la seva naturalesa i pel moment en què es van publicar, aquestes directrius no abordaven totes les qüestions pràctiques amb prou detall. Per tant, ha calgut una *orientació pràctica basada en casos concrets*, que utilitzi les experiències adquirides per les autoritats de control des que l'RGPD és d'aplicació.

3. Aquest document té per finalitat complementar les Directrius WP 250 i reflecteix les experiències comunes de les AC de l'EEE des de l'entrada en vigor l'RGPD. Té com a objectiu ajudar els responsables del tractament a gestionar les violacions de la seguretat de les dades i conèixer quins factors cal tenir en compte a l'hora d'avaluar el risc.

4. Com a part de qualsevol intent d'abordar una violació, en primer lloc el responsable i l'encarregat del tractament l'han de poder reconèixer. L'article 4.12 de l'RGPD defineix la violació de la seguretat de les dades com "qualsevol violació de la seguretat que ocasiona la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses,

[1] Al llarg d'aquest document, les referències a *estats membres* s'han d'entendre com a referències als estats membres de l'EEE (Espai Econòmic Europeu).
[2] COM(2020) 264 final, 24 de juny de 2020.
[3] G29 WP250 rev. 1, 6 de febrer de 2018, Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el Reglament 2016/679 - aprovades pel Comitè Europeu de Protecció de Dades, https://ec.europa.eu/newsroom/article29/items/612052.

conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades."

5. Al Dictamen 03/2014 sobre la notificació de violació de dades personals[4] i les Directrius WP 250, el Grup de treball de l'article 29 explicava que les violacions es poden classificar d'acord amb els següents tres principis de la seguretat de la informació, ben coneguts:

   - Violació de la confidencialitat: quan es produeix una revelació no autoritzada o accidental de les dades personals, o un accés a aquestes dades en idèntiques condicions.
   - Violació de la integritat: quan es produeix una alteració no autoritzada o accidental de les dades personals.
   - Violació de la disponibilitat: quan es produeix una pèrdua d'accés accidental o no autoritzada a les dades personals, o la destrucció d'aquestes dades en idèntiques condicions.[5]

6. Una violació pot comportar diversos efectes adversos significatius per a les persones, que poden produir danys físics, materials i immaterials. L'RGPD explica que això pot incloure la pèrdua de control de les dades personals pròpies, la restricció dels drets, discriminació, robatori d'identitat o frau, pèrdua financera, reversió no autoritzada de la pseudonimització, danys en la reputació i pèrdua de confidencialitat de les dades subjectes a secret professional. També pot comportar altres perjudicis econòmics o socials significatius per a les persones afectades. Una de les obligacions més importants del responsable del tractament és avaluar aquests riscos per als drets i llibertats de les persones interessades i aplicar les mesures tècniques i organitzatives adequades per abordar-los.

7. En conseqüència, l'RGPD exigeix que el responsable del tractament:

   - Documenti qualsevol violació de la seguretat de les dades personals, inclosos els fets que hi estan relacionats, els seus efectes i les mesures correctores adoptades.[6]
   - Notifiqui la violació a l'autoritat de control competent, llevat que sigui improbable que aquesta violació constitueixi un risc per als drets i les llibertats de les persones físiques.[7]
   - Comuniqui la violació de la seguretat de les dades personals als afectats, quan sigui probable que comporti un alt risc per als drets i llibertats de les persones físiques.[8]

8. Les violacions de la seguretat de les dades són problemes en si mateixes, però també poden ser símptomes d'un sistema de seguretat de les dades vulnerable i possiblement obsolet; també poden indicar debilitats del sistema que cal resoldre. Com a principi general, sempre és millor prevenir les violacions de la seguretat anticipant-s'hi, ja que algunes de les seves conseqüències són, per naturalesa, irreversibles. Abans que un responsable del tractament pugui avaluar *plenament* el risc derivat d'una violació ocasionada per algun tipus d'atac, cal identificar-ne la causa principal, a fi de detectar si les vulnerabilitats que van donar peu a l'incident persisteixen i, per tant, es poden continuar aprofitant. En molts casos, el responsable

[4]G29 WP213, 25 de març de 2014, Dictamen 03/2014 sobre la notificació de violació de dades personals, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4
[5]Vegeu les Directrius WP 250, p. 7. Cal tenir en compte que una violació de la seguretat de les dades pot afectar una o més categories, simultàniament o combinades.
[6]Article 33.5 RGPD.
[7]Article 33.1 RGPD.
[8]Article 34.1 RGPD.

del tractament pot determinar que l'incident pot comportar un risc i, consegüentment, s'ha de notificar. En altres casos, no cal esperar a notificar-la fins que el risc i l'impacte relacionats amb la violació de la seguretat de les dades s'hagin avaluat totalment, ja que l'avaluació del risc completa es pot fer paral·lelament a la notificació. D'aquesta manera, es pot proporcionar a l'AC la informació en fases, sense dilació indeguda.[9]

9. La violació s'ha de notificar quan el responsable del tractament considera que és probable que comporti un risc per als drets i les llibertats de la persona afectada. Els responsables han de fer aquesta avaluació en el moment que tinguin coneixement de la violació. No poden esperar a un examen forense detallat i a mesures de mitigació (inicials), abans d'avaluar si és probable que la violació comporti un risc i, en conseqüència, s'ha de notificar.

10. Si el responsable del tractament autoavalua el risc com a improbable, però el risc es materialitza, l'autoritat de control competent pot fer ús de les seves facultats correctores i imposar sancions.

11. Cada responsable i encarregat del tractament ha de tenir establerts plans i procediments per gestionar possibles violacions de la seguretat de les dades. Les organitzacions han de tenir jerarquies clares i persones responsables de determinats aspectes del procés de recuperació.

12. La formació i la conscienciació sobre les qüestions de protecció de dades adreçades al personal del responsable i de l'encarregat del tractament, centrades en la gestió de les violacions de la seguretat de les dades (identificació d'un incident i altres mesures que es poden adoptar, etc.), també són essencials per als responsables i encarregats del tractament. La formació s'ha de repetir periòdicament, d'acord amb el tipus d'activitat de tractament i de les dimensions del responsable del tractament, i ha d'abordar les darreres tendències i alertes procedents de ciberatacs o altres incidents de seguretat.

13. El principi de responsabilitat proactiva i el concepte de protecció de les dades per defecte podrien incorporar una anàlisi que s'integri al *Manual sobre la gestió de les violacions de la seguretat de les dades* del responsable i l'encarregat del tractament, que tingui per objectiu establir els fets per a cada aspecte del tractament en cadascuna de les fases principals de l'operació. Aquesta guia, elaborada prèviament, pot proporcionar una font d'informació molt més ràpida que permetria als responsables i encarregats del tractament mitigar els riscos i complir les seves obligacions sense dilacions indegudes. Això garantiria que, si es produís una violació de la seguretat de les dades, les persones que integren l'organització sabrien què han de fer. Així, l'incident es gestionaria més ràpidament que si no hi haguessin plans o mesures de mitigació.

14. Tot i que els casos que es presenten a continuació són ficticis, es basen en casos típics de l'experiència col·lectiva de les AC en les notificacions de violació de la seguretat de les dades. Les anàlisis es refereixen explícitament als casos examinats, però l'objectiu és proporcionar suport als responsables del tractament a l'hora d'avaluar les seves pròpies violacions de la seguretat de les dades. Qualsevol modificació de les circumstàncies dels casos que es descriuen pot implicar nivells de risc diferents o més significatius que, per tant, requereixin mesures diferents o addicionals. Aquestes directrius estructuren els casos d'acord amb determinades categories de violació (per exemple, els atacs amb programes de segrest

[9] Article 33.4 RGPD.

d'arxius). A l'hora de tractar una determinada categoria de violacions, en cada cas se sol·liciten unes mesures de mitigació concretes. Aquestes mesures no necessàriament es repeteixen en cada anàlisi de cas de la mateixa categoria de violacions. Pel que fa als casos inclosos en la mateixa categoria, només se n'estableixen les diferències. Per tant, el lector ha de llegir tots els casos relacionats amb la categoria de violació de la seguretat per identificar les mesures correctes que ha d'adoptar.

15. La documentació interna d'una violació de la seguretat de les dades és una obligació, independentment dels riscos que porti associats, i s'ha de fer en tots i cadascun dels casos. Els casos que es presenten a continuació intenten aclarir si cal notificar o no la violació a l'AC i comunicar-la a les persones afectades.

2 PROGRAMARI DE SEGREST (*RANSOMWARE*)

16. Una causa freqüent de notificació de violació de la seguretat de les dades és un atac amb programari de segrest patit pel responsable del tractament. En aquests casos, un codi maliciós xifra les dades personals i, després, l'atacant exigeix al responsable del tractament un rescat a canvi del codi de desxifrat. Aquest tipus d'atac normalment es classifica com una violació de la disponibilitat, però sovint també es pot produir una violació de la confidencialitat.

2.1 Cas núm. 01: atac amb programari de segrest amb còpia de seguretat adequada i sense exfiltració

Els sistemes informàtics d'una petita empresa manufacturera van ser objecte d'un atac amb programari de segrest i les dades que hi havia emmagatzemades van quedar xifrades. El responsable del tractament utilitzava xifrat en repòs, de manera que totes les dades a les quals va accedir el programa de segrest estaven xifrades amb un algorisme de xifrat d'última generació. La clau de desxifrat no va quedar compromesa durant l'atac, és a dir que l'atacant no hi va poder accedir ni utilitzar-la indirectament. Per tant, l'atacant només va tenir accés a dades personals xifrades. En particular, ni el sistema de correu electrònic de l'empresa ni els sistemes de clients utilitzats per accedir-hi es van veure afectats. L'empresa recorre als serveis d'una empresa externa de ciberseguretat per investigar l'incident. Hi ha registres que permeten el seguiment dels fluxos de dades que surten de l'empresa (inclòs el correu electrònic de sortida). Després d'analitzar els registres i les dades recollides pels sistemes de detecció implantats per l'empresa, una investigació interna amb suport de l'empresa externa de ciberseguretat va determinar *amb certesa* que l'atacant només va xifrar les dades, sense exfiltrar-les. Els registres no mostren cap flux de sortida de dades en l'interval de l'atac. Les dades personals afectades per la violació es refereixen a clients i empleats de l'empresa, en total unes dotzenes de persones. Hi havia disponible una còpia de seguretat i les dades es van restaurar unes hores després que es produís l'atac. La violació no va comportar conseqüències per al funcionament diari del responsable del tractament. No es van produir endarreriments en el pagament als empleats o en la tramitació de les peticions dels clients.

17. En aquest cas, es complien els elements següents de la definició de violació de la seguretat de les dades: una violació de la seguretat va provocar una alteració il·lícita de les dades personals i un accés no autoritzat a aquestes dades.

2.1.1 Cas núm. 01 - Mesures prèvies i avaluació del risc

18. Com succeeix amb tots els riscos plantejats per actors externs, la probabilitat que un atac amb programari de segrest tingui èxit es pot reduir dràsticament reforçant la seguretat de l'entorn de control de les dades. La majoria d'aquestes violacions es pot evitar garantint que s'han adoptat les mesures de seguretat organitzatives, físiques i tecnològiques adequades. Exemples d'aquestes mesures són una gestió correcta dels pedaços i l'ús d'un sistema adequat de detecció de programes maliciosos. Disposar de còpies de seguretat adequades i separades contribuirà a mitigar les conseqüències d'un atac maliciós, si es produeix. A més, un programa de formació i conscienciació dels empleats en matèria de seguretat ajudarà a evitar i reconèixer aquest tipus d'atac. A la secció 2.5 hi ha una llista de mesures recomanables. Entre aquestes mesures, una de les més importants és la gestió adequada dels pedaços que garanteixi que els sistemes estan actualitzats i que es corregeixen totes les vulnerabilitats conegudes dels sistemes implantats, ja que la majoria dels atacs amb programari de segrest aprofiten vulnerabilitats ben conegudes.

19. En avaluar els riscos, el responsable del tractament ha d'investigar la violació i identificar el tipus de codi maliciós, per comprendre les possibles conseqüències de l'atac. Entre els riscos que cal tenir en compte hi ha el risc que les dades s'hagin exfiltrat sense deixar rastre en els registres dels sistemes.

20. En aquest exemple, l'atacant va accedir a dades personals i la confidencialitat dels textos codificats que contenien dades personals xifrades es va veure compromesa. Tanmateix, l'atacant no pot llegir ni utilitzar les dades que s'hagin exfiltrat, com a mínim en aquell moment. La tècnica de xifrat utilitzada pel responsable del tractament és d'última generació. La clau de desxifrat no es va veure compromesa i, en principi, no es podia determinar per altres mitjans. En conseqüència, els riscos de confidencialitat per als drets i llibertats de les persones físiques es minimitzen, tret que el progrés criptoanalític faci que les dades xifrades siguin intel·ligibles en el futur.

21. El responsable del tractament ha de tenir en compte el risc a què s'exposen les persones a causa de la violació.[10] En aquest cas, sembla que els riscos per als drets i llibertats dels afectats provenen de la manca de disponibilitat de les dades personals, i la confidencialitat de les dades no està compromesa.[11] En aquest exemple, els efectes adversos de la violació es van mitigar poc després que es produís la violació de la seguretat. Disposar d'un sistema de

[10]Per a les orientacions sobre les operacions de tractament "que poden comportar un alt risc", vegeu el document del Grup de treball de l'article 29 *Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) i per determinar si el tractament comporta probablement un alt risc*, als efectes del Reglament 2016/679, WP248 rev. 01, aprovat pel CEPD, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11]Des del punt de vista tècnic, el xifrat de les dades implica l'accés a dades originals i, en el cas de programari de segrest, la supressió de les dades originals: cal accedir a les dades amb un codi maliciós per xifrar-les i eliminar les dades originals. Un atacant pot fer una còpia de l'original abans de suprimir-lo, però les dades personals no sempre s'extrauen. A mesura que la investigació iniciada pel responsable del tractament avança, pot aparèixer més informació que modificarà aquesta avaluació. L'accés que comporta la destrucció, pèrdua, alteració o comunicació no autoritzada de les dades personals o un risc per a la seguretat de la persona afectada, encara que no hi hagi descodificació de les dades personals, pot ser tan greu com l'accés amb descodificació.

còpies de seguretat adequat[12] fa que els efectes de la violació siguin menys greus i, en aquest cas, el responsable del tractament en va poder fer un ús eficaç.

22. Quant a la gravetat de les conseqüències per a les persones afectades, només se'n van poder determinar conseqüències menors, ja que les dades afectades es van restablir en poques hores. Per tant, la violació no va comportar conseqüències per al funcionament diari del responsable del tractament i no va tenir cap efecte significatiu per a les persones afectades (per exemple, pagaments a empleats o gestió de peticions dels clients).

2.1.2 Cas núm. 01 - Mitigació i obligacions

23. Sense una còpia de seguretat, hi ha poques mesures que el responsable pugui adoptar per solucionar la pèrdua de dades personals i cal tornar-les a recollir. Tot i això, en aquest cas concret, els efectes de l'atac es podrien contenir d'una manera eficaç, restablint tots els sistemes compromesos a un estat net i lliure de codi maliciós, corregint les vulnerabilitats i restaurant les dades afectades al més aviat possible després de l'atac. Sense una còpia de seguretat, les dades es perden i la gravetat pot augmentar, perquè els riscos o les repercussions per a les persones afectades també poden ser més greus.

24. La rapidesa en la restauració eficaç de les dades a partir de la còpia de seguretat disponible és una variable clau a l'hora d'analitzar la violació. L'especificació d'un termini adequat per recuperar les dades compromeses depèn de les circumstàncies concretes de la violació. L'RGPD estableix que una violació de la seguretat de les dades personals s'ha de notificar sense dilació indeguda i, si és possible, en el termini màxim de 72 hores. Per tant, es podria concloure que no és aconsellable superar el termini de 72 hores però, quan es tracta de casos considerats d'alt risc, fins i tot complir aquest termini es pot considerar insatisfactori.

25. En aquest cas, després d'una avaluació de l'impacte i d'un procés detallat de resposta a l'incident, el responsable del tractament va determinar que era improbable que la violació comportés un risc per als drets i les llibertats de les persones físiques. En conseqüència, no cal comunicar-la a les persones afectades ni notificar-la a l'AC. Tanmateix, com qualsevol violació de la seguretat de les dades, cal documentar-la d'acord amb el que disposa l'article 33.5 de l'RGPD. L'organització també pot necessitar (o més tard l'AC ho pot requerir) actualitzar i corregir la seva gestió tècnica i organitzativa de la seguretat de les dades personals, així com les seves mesures i procediments de mitigació de riscos. En el marc d'aquesta actualització i correcció, l'organització ha d'investigar exhaustivament la violació i identificar-ne les causes i els mètodes utilitzats per l'atacant, per evitar que es produeixin incidents similars en el futur.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	X	X

[12]Els procediments de còpia de seguretat han de ser estructurats, coherents i repetibles. Exemples de procediments complementaris són el mètode 3-2-1 i el mètode "avi-pare-fill". Qualsevol mètode s'ha de provar en termes de l'eficàcia per cobrir i restaurar les dades. Les proves també s'han de repetir a intervals i, especialment, quan hi ha canvis en l'operació de tractament o les seves circumstàncies, per garantir la integritat del sistema.

2.2 Cas núm. 02: atac amb programari de segrest sense còpia de seguretat adequada

Un dels ordinadors emprats per una empresa agrícola va ser objecte d'un atac amb programari de segrest i l'atacant en va xifrar les dades. L'empresa està utilitzant els coneixements especialitzats d'una empresa externa de ciberseguretat per vigilar la seva xarxa. Els registres que fan el seguiment dels fluxos de dades que surten de l'empresa estan disponibles (inclòs el correu electrònic de sortida). Després d'analitzar els registres i les dades obtingudes pels sistemes de detecció, la investigació interna assistida per l'empresa de ciberseguretat va determinar que l'atacant només va xifrar les dades, sense exfiltrar-les. Els registres no mostren cap flux de dades de sortida en el temps que va durar l'atac. Les dades personals afectades per la violació es refereixen als clients i empleats de l'empresa, en total unes dotzenes de persones. No n'han resultat afectades categories especials de dades. No hi havia còpia de seguretat disponible en format electrònic. La majoria de les dades es van recuperar a partir de còpies de seguretat en paper. La recuperació va trigar 5 dies laborables i va provocar retards menors en el lliurament de les comandes als clients.

2.2.1 Cas núm. 02 - Mesures prèvies i avaluació del risc

26. El responsable del tractament hauria d'haver pres les mesures ja esmentades a la part 2.1 i a la secció 2.9. La diferència principal respecte del cas anterior és que no hi ha còpia de seguretat electrònica ni xifrat de les dades en repòs. Això comporta diferències importants en els passos a seguir.

27. A l'hora d'avaluar aquests riscos, el responsable del tractament ha d'investigar el mètode de d'infiltració i determinar el tipus de codi maliciós, per comprendre les possibles conseqüències de l'atac. En aquest exemple, el programari de segrest va xifrar les dades, sense exfiltrar-les. Així, sembla que els riscos per als drets i llibertats de les persones afectades deriven de la manca de disponibilitat de les dades personals, i la confidencialitat no es veu compromesa. Per determinar el risc, és essencial fer un examen exhaustiu dels registres dels tallafocs i les seves implicacions. El responsable del tractament ha de presentar les conclusions objectives d'aquestes investigacions, si se li demana.

28. Cal que el responsable del tractament tingui en compte que, si l'atac és més sofisticat, el programa maliciós té la funcionalitat d'editar fitxers de registre i eliminar-ne el rastre. Per tant, atès que els registres no s'envien o es reprodueixen en un servidor de registres central, fins i tot després d'una investigació en profunditat que determini que l'atacant no va exfiltrar dades personals, el responsable del tractament no pot afirmar que l'absència d'una anotació al registre demostra que no hi va haver exfiltració. En conseqüència, no es pot descartar totalment la probabilitat d'una violació de la confidencialitat.

29. El responsable del tractament ha d'avaluar els riscos d'aquesta violació,[13] si l'atacant va accedir a les dades. Durant l'avaluació del risc, el responsable del tractament també ha de tenir en compte la naturalesa, la sensibilitat, el volum i el context de les dades personals afectades per la violació. En aquest cas, no hi va haver categories especials de dades personals afectades i la quantitat de dades vulnerades i de persones afectades és baixa.

[13] Per obtenir orientació sobre el tractament que "pot comportar un alt risc", vegeu la nota al peu 10.

30. Per determinar el nivell de risc i prevenir un atac nou o continuat és clau recopilar informació precisa sobre l'accés no autoritzat. Si les dades s'haguessin copiat de la base de dades, això hauria estat un factor d'increment del risc. Quan hi hagi dubtes sobre les característiques específiques de l'accés il·lícit, cal considerar el pitjor escenari i el risc s'ha d'avaluar d'acord amb això.

31. L'absència d'una còpia de seguretat de la base de dades es pot considerar un factor que incrementa el risc, segons la gravetat de les conseqüències per a les persones afectades de la falta de disponibilitat de les dades.

2.2.2 Cas núm. 02 - Mitigació i obligacions

32. Sense una còpia de seguretat, el responsable pot adoptar poques mesures per solucionar la pèrdua de dades personals i cal recollir-les de nou, tret que hi hagi una altra font disponible (per exemple, correus de confirmació de comanda). Sense una còpia de seguretat, les dades es poden perdre i la gravetat dependrà de les conseqüències que això tingui per a les persones afectades.

33. La restauració de les dades no ha de ser excessivament problemàtica,[14] si les dades continuen disponibles en paper. No obstant això, en no haver-hi una còpia de seguretat de la base de dades en format electrònic, es considera necessari notificar la violació a l'AC, ja que la recuperació de les dades pot requerir cert temps i pot causar retards en el lliurament de les comandes als clients. A més, és possible que una quantitat considerable de metadades (per exemple, registres o marques de temps) no es pugui recuperar.

34. La comunicació de la violació a les persones afectades també pot dependre del temps que les dades personals no estiguin disponibles, i de les dificultats que això pot suposar per al funcionament del responsable del tractament (per exemple, endarreriments en la transferència de pagaments als empleats). Atès que els retards en els pagaments i els lliuraments poden desembocar en pèrdues econòmiques per a les persones titulars de les dades compromeses, es podria argumentar que la violació pot comportar un risc alt. A més, pot ser inevitable haver-ne d'informar les persones afectades, si cal la seva col·laboració per recuperar les dades encriptades.

35. Aquest cas exemplifica un atac amb programari de segrest amb risc per als drets i llibertats de les persones afectades, però que no arriba al nivell de risc alt. Cal documentar-lo d'acord amb el que disposa l'article 33.5 i notificar-lo a l'AC, d'acord amb el que estableix l'article 33.1. L'organització també pot necessitar (o l'AC li pot requerir) actualitzar i corregir la seva gestió tècnica i organitzativa de la seguretat de les dades personals i les mesures i procediments de mitigació del risc.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	X

[14] Això dependrà de la complexitat i estructura de les dades personals. En els escenaris més complexos, per restablir la integritat de les dades i la coherència amb les metadades, poden caldre recursos i esforços importants per garantir les relacions correctes dins de les estructures de dades i comprovar-ne la precisió.

2.3 Cas núm. 03: atac amb programari de segrest en un hospital, amb còpia de seguretat i sense exfiltració

El sistema d'informació d'un hospital/centre sanitari va ser objecte d'un atac amb programari de segrest i l'atacant en va encriptar una part significativa de les dades. L'empresa està utilitzant els serveis d'una empresa externa de ciberseguretat per controlar la seva xarxa. Els registres que permeten el seguiment dels fluxos de dades que surten de l'empresa estan disponibles (inclòs el correu electrònic de sortida). Després d'analitzar els registres i les dades obtingudes pels sistemes de detecció, la investigació interna assistida per l'empresa de ciberseguretat ha determinat que l'atacant només va xifrar les dades, sense exfiltrar-les. Els registres no mostren cap flux de sortida de dades en el temps que va durar l'atac. Les dades personals afectades per la violació es refereixen a empleats i pacients, cosa que suposa milers de persones. Hi havia còpies de seguretat disponibles en format electrònic. La majoria de les dades es van recuperar, però van caldre 2 dies laborables i això va comportar endarreriments importants en el tractament per als pacients als quals es van cancel·lar o ajornar cirurgies, i una reducció del nivell de servei a causa de la manca de disponibilitat dels sistemes.

2.3.1 Cas núm. 03 - Mesures prèvies i avaluació del risc

36. El responsable del tractament hauria d'haver adoptat les mesures prèvies ja esmentades a la part 2.1 i a la secció 2.5. La principal diferència amb el cas anterior és la important gravetat de les conseqüències per a una part substancial de les persones afectades.[15]

37. La quantitat de dades afectades i el nombre de les persones afectades és elevat, perquè els hospitals acostumen a tractar grans volums de dades. La falta de disponibilitat de les dades té un gran impacte en una part significativa de les persones afectades. A més, hi ha un risc residual d'alta gravetat per a la confidencialitat de les dades dels pacients.

38. El tipus de violació, la naturalesa, la sensibilitat i el volum de dades personals afectades són importants. Encara que hi hagi una còpia de seguretat i les dades es puguin restaurar en uns dies, hi persisteix un alt risc a causa de la gravetat de les conseqüències per a les persones afectades derivada de la falta de disponibilitat de les dades en el moment de l'atac i els dies següents.

2.3.2 Cas núm. 03 - Mitigació i obligacions

39. Es considera que cal notificar la violació a l'AC, ja que es tracta de categories especials de dades i la recuperació de les dades pot requerir molt de temps, cosa que comportaria importants retards en l'atenció al pacient. Cal informar les persones afectades sobre la violació, atès l'impacte que té en els pacients fins i tot un cop recuperades les dades encriptades. Si bé s'han encriptat les dades relatives a tots els pacients que s'han tractat a l'hospital durant els últims anys, només se n'han vist afectats els pacients que tenien programat un tractament a l'hospital durant el temps en què el sistema informàtic no va estar disponible. El responsable del tractament ha de comunicar la violació de la seguretat de les dades a aquests pacients directament. La comunicació directa a la resta de pacients, alguns

[15]Per obtenir informació sobre el tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

dels quals no han estat a l'hospital des de fa més de vint anys, pot no ser necessària a causa de l'excepció prevista a l'article 34.3.*c*. En aquest cas, en lloc d'això s'ha d'optar per una comunicació pública[16] o una mesura similar que informi les persones afectades d'una manera igualment efectiva. En aquest cas, l'hospital ha de fer públics l'atac amb programari de segrest i els seus efectes.

40. Aquest cas exemplifica un atac amb programari de segrest amb risc per als drets i llibertats de les persones afectades. Cal documentar-lo d'acord amb el que disposa l'article 33.5, notificar-lo a l'autoritat de control segons el que estableix l'article 33.1 i comunicar-lo a les persones afectades d'acord amb l'article 34.1. L'organització també ha d'actualitzar i corregir la seva gestió tècnica i organitzativa de la seguretat de les dades personals i les seves mesures i procediments de mitigació de riscos.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones interessades
✓	✓	✓

2.4 Cas núm. 04: atac amb programari de segrest sense còpia de seguretat adequada i amb exfiltració

El servidor d'una empresa de transport públic va ser objecte d'un atac amb programari de segrest i l'atacant en va xifrar les dades. Segons les conclusions de la investigació interna, l'atacant va encriptar les dades i, a més, les va exfiltrar. Les dades afectades eren de clients i empleats, així com dels diversos milers de persones usuàries dels serveis de l'empresa (per exemple, que compraven bitllets en línia). A més de les dades bàsiques identificatives, la violació ha afectat els números dels documents d'identitat i dades financeres, com ara les de targetes de crèdit. Hi havia una còpia de seguretat de la base de dades, però l'atacant també la va xifrar.

2.4.1 Cas núm. 04 - Mesures prèvies i avaluació del risc

41. El responsable del tractament hauria d'haver adoptat les mesures ja esmentades a la part 2.1 i a la secció 2.5. Hi havia una còpia de seguretat, però també va resultar afectada per l'atac. Aquest sistema per si sol qüestiona la qualitat de les mesures de seguretat informàtica prèvies del responsable del tractament i cal examinar-les amb més detall durant la investigació, ja que, en un sistema de còpies de seguretat ben dissenyat, les múltiples còpies de seguretat s'han d'emmagatzemar de forma segura sense que s'hi pugui accedir des del sistema principal. En cas contrari, aquestes còpies poden quedar compromeses en el mateix atac. A més, els atacs amb programari de segrest poden estar ocults durant dies i anar encriptant lentament dades que rarament s'utilitzen. Això pot inutilitzar les múltiples còpies de seguretat, per la qual cosa cal fer-les periòdicament i aïllar-les. Això augmentaria les probabilitats de recuperació, encara que es perdessin més dades.

[16]Segons el considerant 86 de l'RGPD, "Aquestes comunicacions als afectats s'han de fer tan aviat com sigui raonablement possible i en estreta cooperació amb l'autoritat de control, seguint les seves orientacions o les d'altres autoritats competents, com les autoritats policials. Així, per exemple, la necessitat de mitigar un risc de danys i perjudicis immediats justificaria una ràpida comunicació a les persones afectades, mentre que la necessitat d'aplicar mesures adequades per impedir violacions de la seguretat de les dades personals contínues o similars pot justificar que la comunicació porti més temps."

42. Aquesta violació de la seguretat no afecta únicament la disponibilitat de les dades. També n'afecta la confidencialitat, ja que l'atacant pot haver modificat o copiat dades del servidor. Per tant, el tipus de violació comporta un alt risc.[17]

43. La naturalesa, la sensibilitat i el volum de les dades personals incrementa el risc, ja que el nombre de persones afectades és més alt, igual com la quantitat global de dades personals afectades. A més de les dades bàsiques identificatives, també han resultat afectades per la violació els documents d'identitat i dades financeres, com ara les de targetes de crèdit. Una violació de la seguretat de les dades que afecti aquests tipus de dades suposa un gran risc en si mateixa i, si es tracten conjuntament, es poden utilitzar per a la suplantació d'identitat o frau, entre altres coses.

44. A causa d'una lògica del servidor o d'uns controls organitzatius defectuosos, els fitxers de la còpia de seguretat es van veure afectats pel programari de segrest, cosa que va impedir recuperar les dades i el risc va augmentar.

45. Aquesta violació de la seguretat de les dades comporta un risc alt per als drets i llibertats de les persones, ja que podria provocar danys materials (com ara pèrdues econòmiques, ja que les dades de la targeta de crèdit estarien afectades) i immaterials (per exemple, suplantació d'identitat o frau, ja que les dades del document d'identitat estarien afectades).

2.4.2 Cas núm. 04 - Mitigació i obligacions

46. La comunicació a les persones afectades és essencial perquè puguin prendre les mesures necessàries per evitar perjudicis importants (per exemple, bloquejar les seves targetes de crèdit).

47. A banda de documentar la violació d'acord amb l'article 33.5, en aquest cas la notificació a l'AC és obligatòria (article 33.1) i el responsable del tractament també l'ha de comunicar a les persones afectades (article 34.1). Aquesta comunicació pot ser individualitzada però, si no es tenen les dades de contacte de les persones afectades, el responsable del tractament ho ha de fer públicament, per exemple amb una comunicació al seu lloc web. Això, sempre que aquesta comunicació no comporti conseqüències negatives addicionals per a les persones afectades. Aquesta comunicació ha de ser precisa i clara, visible a simple vista a la pàgina d'inici del responsable del tractament, amb referències exactes al que estableix l'RGPD. L'organització potser també ha d'actualitzar i corregir la seva gestió tècnica i organitzativa de la seguretat de les dades personals, així com les seves mesures i procediments de mitigació del risc.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones interessades
✓	✓	✓

[17] Per obtenir informació sobre el tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

2.5 Mesures tècniques i organitzatives per prevenir o mitigar l'impacte dels atacs amb programari de segrest

48. El fet que s'hagi produït un atac amb programari de segrest acostuma a indicar que hi ha una o més vulnerabilitats en el sistema del responsable del tractament. Això també s'aplica als casos de programes de segrest en què les dades personals s'han encriptat, però no s'han exfiltrat. Sigui quin sigui el resultat i les conseqüències de l'atac, no s'insistirà mai prou en la importància d'una avaluació global del sistema de seguretat de les dades, amb especial èmfasi en la seguretat informàtica. Les deficiències detectades s'han de documentar i resoldre immediatament.

49. Mesures recomanables:

    (La següent llista de mesures no és exclusiva o completa. Al contrari, té per objectiu aportar idees per a la prevenció i possibles solucions. Cada activitat de tractament és diferent, per la qual cosa el responsable del tractament ha de decidir quines mesures són més adequades d'acord amb la situació.)

    - Mantenir actualitzats el microprogramari (*firmware*), el sistema operatiu i el programari d'aplicació en els servidors, màquines client, components de xarxa actius i altres màquines de la mateixa LAN (inclosos els dispositius wifi). Assegurar que s'apliquen les mesures de seguretat informàtica adequades, garantir que són efectives i actualitzar-les periòdicament, quan el tractament o les circumstàncies canviïn o evolucionin. Això inclou conservar registres detallats sobre les revisions que s'apliquen, i en quina data.
    - Dissenyar i organitzar els sistemes de tractament i les infraestructures per segmentar o aïllar les xarxes i els sistemes de dades, per evitar la propagació de programari maliciós a la mateixa organització i a sistemes externs.
    - Tenir un procediment de còpies de seguretat actualitzat, segur i provat. Els suports on s'emmagatzemen les còpies de seguretat de llarg i mitjà termini han d'estar separats dels suports d'emmagatzematge de dades operatives i fora de l'abast de tercers, fins i tot en cas d'un atac amb èxit (per exemple, amb còpies de seguretat incrementals diàries i còpies de seguretat completes setmanals).
    - Tenir/adquirir un programari adequat, actualitzat, eficaç i integrat contra els programes maliciosos.
    - Disposar d'un sistema de tallafocs i prevenció d'intrusions adequat, actualitzat, eficaç i integrat. Dirigir el trànsit de la xarxa al tallafocs / a la detecció d'intrusió, fins i tot en els equips de teletreball o mòbil (per exemple, utilitzant connexions VPN als mecanismes de seguretat de l'organització en accedir a internet).
    - Formar els empleats sobre els mètodes per reconèixer i prevenir els atacs informàtics. El responsable ha de proporcionar mitjans per determinar si els correus electrònics i missatges obtinguts per altres mitjans de comunicació són autèntics i de confiança. Cal formar els empleats perquè puguin reconèixer quan s'ha produït un atac d'aquest tipus, com desconnectar el terminal de la xarxa i l'obligació d'informar-ne immediatament el responsable de seguretat.
    - Insistir en la necessitat d'identificar el tipus de codi maliciós per veure les conseqüències de l'atac i poder trobar les mesures adequades per mitigar-ne el risc. Si un atac amb

programari de segrest ha assolit el seu objectiu i no hi ha còpies de seguretat disponibles, es poden emprar eines com les proporcionades pel projecte «no more ransom» (nomoreransom.org) per recuperar les dades. Tanmateix, si hi ha una còpia de seguretat segura, és recomanable restaurar les dades a partir d'aquesta còpia.

- Reenviament o rèplica de tots els registres a un servidor de registres central (possiblement incloent-hi la firma o la marca de temps criptogràfica de les entrades de registre).
- Xifrat d'alta seguretat i autenticació de múltiples factors, en particular per a l'accés administratiu als sistemes informàtics i la gestió adequada de claus i contrasenyes.
- Proves de vulnerabilitat i penetració periòdicament.
- Crear un equip de resposta davant d'incidents de seguretat informàtica (CSIRT) o un equip de resposta a emergències informàtiques (CERT) dins de l'organització, o adherir-se a un CSIRT/CERT col·lectiu. Crear un pla de resposta davant d'incidents, un pla de recuperació de desastres i un pla de continuïtat de les activitats, i assegurar-se que se sotmeten a proves exhaustives.
- A l'hora d'avaluar les contramesures, l'anàlisi de riscos s'ha de revisar, provar i actualitzar.

3 ATACS AMB EXFILTRACIÓ DE DADES

50. Els atacs que aprofiten les vulnerabilitats dels serveis que el responsable del tractament presta a tercers per internet, per exemple amb atacs d'injecció (injecció SQL o rutes transversals) que comprometen el lloc web i mètodes similars, es poden assemblar a atacs amb programari de segrest perquè el risc prové de l'acció d'un tercer no autoritzat. Però normalment l'objectiu d'aquests atacs és copiar, exfiltrar i utilitzar les dades personals amb alguna finalitat maliciosa. Per tant, són principalment violacions de la confidencialitat i, possiblement, també violacions de la integritat de les dades. Alhora, si el responsable del tractament coneix les característiques d'aquest tipus de violacions, hi ha moltes mesures que poden reduir substancialment el risc que l'atac tingui èxit.

3.1 Cas núm. 05: exfiltració de les dades de sol·licituds d'ocupació d'un lloc web

Una oficina d'ocupació va ser víctima d'un ciberatac, que va inserir un codi maliciós al seu lloc web. Aquest codi maliciós va fer accessible a persones no autoritzades la informació personal enviada a través dels formularis de sol·licitud d'ocupació en línia i emmagatzemada al servidor web. És probable que 213 d'aquests formularis estiguin afectats. Després d'analitzar les dades afectades, es va determinar que no hi havia categories especials de dades afectades per la violació. Les eines malicioses instal·lades tenien funcionalitats que permetien a l'atacant eliminar qualsevol historial d'exfiltració i, també, monitorar el tractament que tenia lloc al servidor i capturar les dades personals. El programari maliciós es va descobrir al cap d'un mes d'haver estat instal·lat.

3.1.1 Cas núm. 05 - Mesures prèvies i avaluació del risc

51. La seguretat de l'entorn del responsable del tractament és summament important, ja que la majoria d'aquestes violacions es poden evitar garantint que tots els sistemes estan permanentment actualitzats, que les dades confidencials estan xifrades i que les aplicacions

s'han desenvolupat d'acord amb alts estàndards de seguretat, com ara autenticació segura, mesures contra la força bruta, atacs, "escapada" o "sanejament"[18] de les dades introduïdes per ususaris, etc. Per detectar aquest tipus de vulnerabilitats prèviament i corregir-les, també cal fer auditories periòdiques de seguretat informàtica, avaluacions de vulnerabilitats i proves de penetració. En aquest cas concret, tenir eines de vigilància de la integritat dels fitxers a l'entorn de producció podria haver ajudat a detectar la injecció de codi (a la secció 3.7 hi ha una llista de mesures recomanables).

52. El responsable del tractament sempre ha de començar a investigar la violació identificant el tipus i mètodes de l'atac, per avaluar quines mesures cal adoptar. Per fer-ho de manera ràpida i eficaç, el responsable ha de tenir implantat un pla de resposta a incidents, que especifiqui les mesures ràpides i necessàries per controlar l'incident. En aquest cas concret, el tipus de violació era un factor que incrementava el risc, ja que no només va afectar la confidencialitat de les dades, sinó que l'atacant tenia mitjans per fer canvis en el sistema, de manera que la integritat de les dades també era qüestionable.

53. Per determinar l'afectació per a les persones interessades, cal avaluar la naturalesa, sensibilitat i quantitat de dades personals afectades. Tot i que no hi havia dades de categories especials afectades, les dades a les quals s'havia accedit contenien una informació considerable sobre les persones, obtinguda dels formularis en línia, i aquestes dades es podrien utilitzar indegudament de diverses maneres (selecció de destinataris de màrqueting no sol·licitat, usurpació d'identitat, etc.). Per tant, la gravetat de les conseqüències augmenta el risc per als drets i les llibertats de les persones interessades.[19]

3.1.2 Cas núm. 05 - Mitigació i obligacions

54. Si és possible, un cop resolt el problema, les bases de dades s'han de comparar amb la còpia de seguretat emmagatzemada de manera segura. L'experiència adquirida a partir de la violació s'ha d'utilitzar a l'hora d'actualitzar la infraestructura informàtica. El responsable del tractament ha de retornar tots els sistemes informàtics afectats a un estat net conegut, corregir la vulnerabilitat i aplicar noves mesures de seguretat per evitar violacions de seguretat similars en el futur, com ara controls d'integritat dels fitxers i auditories de seguretat. Si les dades personals no només es van exfiltrar, sinó que també es van suprimir, el responsable del tractament ha d'adoptar mesures sistemàtiques per recuperar les dades personals i restaurar-les a l'estat previ a la violació. Pot caldre fer còpies de seguretat completes, canvis incrementals i després, possiblement, tornar a executar el tractament des de l'última còpia de seguretat incremental. Això requereix que el responsable pugui repetir els canvis efectuats des de l'última còpia de seguretat, cosa que pot exigir que tingui un sistema dissenyat per conservar els fitxers d'introducció de dades diàries, per si s'han de tornar a tractar, i requereix també un mètode d'emmagatzematge sòlid i una política de conservació adequada.

55. En vista de l'anterior, ja que és probable que la violació comporti un risc alt per als drets i llibertats de les persones físiques, cal comunicar-la a les persones afectades (article 34.1). Òbviament, això significa que l'autoritat de control competent també s'hi ha d'implicar, amb

[18] L'escapada o el sanejament de les dades introduïdes pels usuaris és una forma de validació que garanteix que en un sistema d'informació només hi entren les dades amb un format adequat.
[19] Per a més informació sobre el tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

una notificació de violació de la seguretat de les dades. D'acord amb l'article 33.5 de l'RGPD, és obligatori documentar la violació, cosa que facilita l'avaluació de la situació.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'AC	Comunicació a les persones afectades
✓	✓	✓

3.2 Cas núm. 06 - Exfiltració d'una contrasenya xifrada des d'un lloc web

Es va aprofitar una vulnerabilitat d'injecció SQL per accedir a la base de dades del servidor d'un lloc web de cuina. Els usuaris només podien triar pseudònims arbitraris com a nom d'usuari. Es recomanava no fer ús d'adreces electròniques amb aquesta finalitat. Les contrasenyes emmagatzemades a la base de dades es van xifrar amb un algorisme fort i el salt [transmissions de dades intermèdies entre dos nodes de comunicacions consecutius] no es va veure compromès. Dades afectades: contrasenyes xifrades de 1.200 usuaris. Per a més seguretat, el responsable del tractament va comunicar la violació a les persones afectades, per correu electrònic, i els va demanar que canviessin les contrasenyes, especialment si s'emprava la mateixa contrasenya per a d'altres serveis.

3.2.1 Cas núm. 06 - Mesures prèvies i avaluació del risc

56. En aquest cas concret, la confidencialitat de les dades queda afectada, però les contrasenyes de la base de dades es van xifrar amb funcions *hash* amb un mètode actualitzat i això disminuiria el risc pel que fa a la naturalesa, sensibilitat i volum de dades personals. Aquest cas no comporta riscos per als drets i llibertats de les persones afectades.

57. A més, no es va posar en risc la informació de contacte de les persones afectades (com ara adreces electròniques o números de telèfon), cosa que significa que no hi ha un risc substancial que les persones interessades siguin objecte d'intents de frau (per exemple, amb correus electrònics de suplantació d'identitat [*phishing*] o trucades telefòniques i missatges de text fraudulents). No s'hi han vist afectades categories especials de dades.

58. Alguns noms d'usuari es podrien considerar dades personals, però la matèria que tracta el lloc web no permet connotacions negatives. Això no obstant, l'avaluació del risc pot canviar,[20] si el tipus de lloc web i les dades a les quals s'ha accedit poden revelar categories especials de dades (per exemple, el lloc web d'un partit polític o d'un sindicat). Fer servir el xifratge més avançat podria mitigar els efectes adversos de la violació. Així mateix, garantir que es permet un nombre limitat d'intents per iniciar de sessió evitarà que els atacs de connexió per força bruta tinguin èxit, amb la qual cosa es redueixen significativament els riscos que suposa que els atacants ja coneguin els noms d'usuari.

[20]Per obtenir informació sobre el tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

3.2.2 Cas núm. 06 - Mitigació i obligacions

59. En alguns casos, la comunicació a les persones afectades es podria considerar un atenuant, ja que llavors estan en condicions de prendre les mesures necessàries per evitar altres danys derivats de la violació, com ara canviar la contrasenya. En aquest cas la notificació no era obligatòria, però en molts casos es pot considerar una bona pràctica.

60. El responsable del tractament ha de corregir la vulnerabilitat i aplicar noves mesures de seguretat per evitar violacions de la seguretat de les dades similars en el futur, com ara auditories sistemàtiques de seguretat del lloc web.

61. La violació s'ha de documentar d'acord amb l'article 33.5, però no cal notificar-la ni comunicar-la als afectats.

62. També és molt recomanable comunicar a les persones afectades una violació de la seguretat de les contrasenyes en qualsevol cas, fins i tot quan les contrasenyes s'emmagatzemen mitjançant un *hash* amb valors de salt amb un algorisme d'acord amb la tècnica més avançada. És preferible fer servir mètodes d'autenticació que evitin la necessitat que el servidor processi contrasenyes. Cal oferir a les persones afectades la possibilitat de prendre les mesures adequades en relació amb les pròpies contrasenyes.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	X	X

3.3 Cas núm. 07 - Atac de reutilització de credencials en un lloc web bancari

Un banc va patir un ciberatac contra un dels seus llocs web de banca en línia. L'atac tenia com a objectiu fer un llistat de tots els identificadors d'usuari, utilitzant una contrasenya trivial fixa. Les contrasenyes són de 8 dígits. A causa d'una vulnerabilitat del lloc web, en alguns casos es va filtrar a l'atacant informació relativa a les persones afectades (nom, cognom, sexe, data i lloc de naixement, codi fiscal, codis d'identificació d'usuari), fins i tot si la contrasenya utilitzada no era correcta o si el compte bancari ja no estava actiu. Hi va haver aproximadament 100.000 persones afectades. D'aquestes, l'atacant va es connectar amb èxit a uns 2.000 comptes que utilitzaven la contrasenya trivial que havia provat. Després d'això, el responsable del tractament va poder identificar tots els intents il·legítims d'inici de sessió i va poder confirmar que, d'acord amb les verificacions antifrau, aquests comptes no van fer transaccions durant l'atac. El banc era conscient de la violació de les dades perquè el seu centre d'operacions de seguretat va detectar un elevat nombre de sol·licituds d'inici de sessió adreçades al lloc web. Com a resposta, el responsable del tractament va desactivar la possibilitat d'iniciar sessió al lloc web i va forçar el canvi de contrasenya dels comptes compromesos. El responsable del tractament només va comunicar la violació als usuaris dels comptes compromesos, és a dir, als usuaris les contrasenyes dels quals havien quedat compromeses o dels quals s'havien divulgat les dades.

3.3.1 Cas núm. 07 - Mesures prèvies i avaluació de risc

63. Cal esmentar que els responsables que tracten dades de caràcter molt personal[21] tenen més responsabilitat pel que fa a proporcionar una seguretat adequada a les dades; per exemple, poden disposar d'un centre d'operacions de seguretat i altres mesures de prevenció, detecció i resposta davant d'incidents. El fet de no complir aquestes normes estrictes sens dubte comportarà mesures més serioses durant una investigació de l'AC.

64. La violació afecta dades financeres que van més enllà de la identitat i la identificació de l'usuari, per la qual cosa és especialment greu. El nombre de persones afectades és alt.

65. El fet que es pugui produir una violació en un entorn tan sensible apunta a importants vulnerabilitats de seguretat en el sistema del responsable del tractament, i pot ser indicatiu d'un moment en què resulta "necessari" revisar i actualitzar les mesures afectades, d'acord amb l'article 24.1, l'article 25.1 i l'article 32.1 de l'RGPD. Les dades vulnerades permeten la identificació única de les persones afectades i contenen més informació sobre elles (inclosos el sexe i el lloc i data de naixement). A més, l'atacant les pot utilitzar per obtenir les contrasenyes dels clients o per dur a terme una campanya de suplantació d'identitat adreçada als clients del banc.

66. Per això, es va considerar que en aquest cas la violació de la seguretat de les dades podia comportar un risc alt per als drets i llibertats de les persones afectades.[22] Per tant, el fet que es produeixin danys materials (com ara pèrdues econòmiques) i immaterials (com ara usurpació d'identitat o frau) és un resultat esperable.

3.3.2 Cas núm. 07 - Mitigació i obligacions

67. Les mesures del responsable del tractament esmentades a la descripció del cas són adequades. Arran de la violació, també va corregir la vulnerabilitat del lloc web i va prendre altres mesures per evitar violacions similars en el futur, com ara implantar l'autenticació de doble factor al lloc web afectat i passar a una autenticació de client més segura.

68. En aquest escenari, documentar la violació d'acord amb l'article 33.5 de l'RGPD i notificar-la a l'autoritat de control no és opcional. A més, d'acord amb l'article 34 de l'RGPD, el responsable del tractament l'ha de comunicar a les 100.000 persones afectades (inclosos els afectats que no tenien els comptes compromesos).

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓

[21] Com ara informació de les persones afectades referida a números de targeta, comptes bancaris, pagament en línia, nòmines, extractes bancaris, estudis econòmics o altra informació susceptible de revelar informació financera relativa als afectats.
[22] Per a més informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

3.4 Mesures tècniques i organitzatives per prevenir o mitigar els efectes dels ciberatacs

69. Igual com en el cas d'atacs amb programari de segrest, independentment del resultat i de les conseqüències de l'atac, els responsables del tractament tenen l'obligació de reavaluar la seguretat informàtica.

70. Mesures recomanables:[23]

    (La llista següent de mesures no es proposa com a exclusiva o completa. Al contrari, té l'objectiu d'aportar idees per a la prevenció i possibles solucions. Cada activitat de tractament és diferent, per la qual cosa el responsable del tractament ha de decidir quines mesures són més adequades en aquella situació.)

    - Gestió de claus i xifrat d'última generació, especialment quan es tracten contrasenyes o dades sensibles o financeres. Per a la informació secreta (contrasenyes), sempre és preferible el *hashejat* i salat criptogràfic, abans que el xifratge. És preferible emprar mètodes d'autenticació que evitin la necessitat que el servidor tracti contrasenyes.

    - Manteniment actualitzat del sistema (programari i microprogramari [*firmware*]). Assegurar que s'han implementat les mesures de seguretat informàtica, garantir que són eficaces i actualitzar-les periòdicament, quan el tractament o les circumstàncies canviïn o evolucionin. Per poder demostrar que compleix l'article 5.1.*f*, d'acord amb l'article 5.2 de l'RGPD el responsable del tractament ha de mantenir un registre de totes les actualitzacions efectuades, inclòs el moment en què es van fer.

    - Ús de mètodes d'autenticació segurs, com ara l'autenticació de doble factor i servidors d'autenticació, complementats amb una política de contrasenyes actualitzada.

    - Els estàndards de desenvolupament segur inclouen el filtrat de les dades introduïdes per l'usuari (utilitzant llistes blanques sempre que sigui viable), l'escapada de les entrades dels usuaris i mesures de prevenció contra la força bruta (com ara la limitació de la quantitat màxima de reintents). Els "tallafocs d'aplicació web" poden contribuir a l'ús eficaç d'aquesta tècnica.

    - Aplicació de privilegis d'usuari segurs i d'una política de gestió del control d'accessos.

    - Ús de tallafocs adequats, actualitzats, eficaços i integrats, detecció d'intrusions i altres sistemes de seguretat perimetrals.

    - Auditories de seguretat informàtica i avaluacions de vulnerabilitat (proves de penetració) sistemàtiques.

    - Revisions i proves periòdiques per garantir que es puguin fer servir les còpies de seguretat per recuperar les dades que hagin vist afectada la seva integritat o disponibilitat.

    - No utilitzar identificador de sessió en URL en text sense format.

[23] Per a un desenvolupament segur de les aplicacions web, vegeu també: https://www.owasp.org/index.php/Main_Page.

4 FONT INTERNA DE RISC HUMÀ

71. Cal destacar el paper de l'error humà en les violacions de la seguretat de les dades personals, ja que es produeix amb freqüència. Com que aquest tipus de violacions poden ser tant intencionats com no intencionats, és difícil per als responsables del tractament identificar les vulnerabilitats i adoptar mesures per evitar-les. La Conferència Internacional d'Autoritats de Protecció de Dades i Privacitat va reconèixer la importància del factor humà, i va adoptar la resolució d'abordar el paper de l'error humà en les violacions de la seguretat de les dades personals l'octubre del 2019.[24] La resolució incideix en la necessitat d'adoptar mesures de protecció adequades per evitar els errors humans i facilita una llista no exhaustiva d'aquests mètodes i salvaguardes.

4.1 Cas núm. 08: exfiltració de dades empresarials per part d'un empleat

Durant el període de notificació prèvia de l'acomiadament, l'empleat d'una empresa copia dades comercials contingudes a la base de dades de l'empresa. L'empleat només està autoritzat a accedir a les dades per complir les seves funcions laborals. Mesos més tard, després d'haver deixat la feina, empra les dades obtingudes (dades bàsiques de contacte) per alimentar un nou tractament de dades del qual és el responsable, amb la finalitat de posar-se en contacte amb els clients de l'empresa i atreure'ls cap a la seva nova activitat.

4.1.1 Cas núm. 08 - Mesures prèvies i avaluació del risc

72. En aquest cas concret, no s'havien adoptat mesures prèvies per evitar que l'empleat copiés la informació de contacte dels clients de l'empresa, ja que necessitava aquest accés per desenvolupar les seves tasques laborals i, en conseqüència, hi tenia accés legítim. Atès que el desenvolupament de la majoria dels llocs de treball relacionats amb clients requereix que els empleats accedeixin a dades personals, aquest tipus de violacions poden ser les més difícils d'evitar. Les limitacions de l'abast de l'accés poden limitar la tasca que l'empleat pot dur a terme. Tanmateix, unes polítiques d'accés ben dissenyades i un control constant poden ajudar a evitar aquestes violacions.

73. Com és habitual, durant l'avaluació del risc cal tenir en compte el tipus de la violació i la naturalesa, sensibilitat i volum de les dades personals afectades. Aquests tipus de violacions acostumen a afectar la confidencialitat, ja que normalment la base de dades queda intacta i el contingut "simplement" es copia per fer-lo servir posteriorment. A més, el volum de dades afectades sol ser baix o mitjà. En aquest cas concret, no es van veure afectades categories especials de dades, ja que l'empleat només necessitava les dades de contacte dels clients, per poder-s'hi posar en contacte després d'haver abandonat l'empresa. Per tant, les dades afectades no són sensibles.

74. Si bé l'únic objectiu de l'exempleat que va copiar les dades maliciosament es pot limitar a aconseguir la informació de contacte dels clients de l'empresa per als seus fins comercials propis, el responsable del tractament no està en condicions de considerar que el risc per a les

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

persones afectades és baix, ja que no té cap garantia sobre les intencions de l'empleat. Així doncs, tot i que les conseqüències de la violació es poden limitar a l'exposició a automàrqueting no sol·licitat, no es pot descartar un altre ús indegut, i més greu, de les dades robades, segons la finalitat del tractament que dugui a terme l'exempleat.[25]

4.1.2 Cas núm. 08 - Mitigació i obligacions

75. És difícil mitigar els efectes adversos de la violació a què es refereix el cas anterior. És probable que calguin accions legals immediates per evitar que l'antic empleat faci un ús indegut de les dades i les divulgui. Com a pas següent, l'objectiu ha de ser evitar situacions similars en el futur. El responsable del tractament podria intentar ordenar a l'antic empleat que deixi d'utilitzar les dades, però en el millor dels casos l'èxit d'aquesta acció és dubtós. La impossibilitat de copiar o descarregar les dades en dispositius extraïbles podria ser útil, entre les possibles mesures tècniques adequades.

76. No hi ha una solució única per a aquests tipus de casos, però un enfocament sistemàtic pot ajudar a evitar-los. Per exemple, l'empresa podria sospesar la possibilitat, quan sigui possible, de retirar determinats tipus d'accés als empleats que han manifestat la intenció de marxar de l'empresa, per poder registrar i marcar l'accés no desitjat. El contracte signat amb els empleats ha d'incloure clàusules que prohibeixin aquestes accions.

77. En resum, atès que la violació en qüestió no comportarà un risc alt per als drets i llibertats de les persones físiques, n'hi haurà prou de notificar-la a l'AC. No obstant això, informar-ne les persones afectades també pot beneficiar el responsable del tractament, ja que segurament és millor que se n'assabentin per l'empresa, en lloc d'assabentar-se'n per l'empleat que intenta posar-s'hi en contacte. D'acord amb l'article 33.5, és obligatori documentar la violació de la seguretat de les dades.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones interessades
✓	✓	X

[25]Per obtenir informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

4.2 Cas núm. 09: transmissió accidental de dades a un tercer de confiança

Un agent d'assegurances es va adonar que podia accedir a informació relacionada amb dues dotzenes de clients aliens al seu àmbit, a causa de la configuració defectuosa d'un fitxer d'Excel rebut per correu electrònic. Està subjecte al secret professional i és l'única persona que va rebre el correu electrònic. L'acord entre el responsable del tractament i l'agent d'assegurances obliga aquest últim a comunicar una violació de la seguretat de les dades personals al responsable del tractament, sense dilació indeguda. Per tant, l'agent va informar-ne immediatament el responsable del tractament, que va corregir el fitxer, el va tornar a enviar i va demanar a l'agent que eliminés el missatge anterior. Segons l'acord esmentat, l'agent ha de confirmar l'eliminació amb una declaració escrita, i així ho va fer. La informació obtinguda no inclou categories especials de dades personals, sinó únicament dades de contacte i dades sobre l'assegurança (tipus d'assegurança, import). Després d'analitzar les dades personals afectades per la violació, el responsable del tractament no va identificar cap característica especial pel que fa a les persones o al responsable del tractament que pogués incidir en el nivell d'impacte de la violació.

4.2.1 Cas núm. 09 - Mesures prèvies i avaluació del risc

78. En aquest cas, la violació no és fruit d'una acció intencionada d'un empleat, sinó d'un error humà no intencionat causat per la falta d'atenció. Aquests tipus de violacions es poden evitar o fer menys freqüents amb: a) l'aplicació de programes de formació i sensibilització perquè els empleats es conscienciïn de la importància de la protecció de les dades personals; b) la reducció de l'intercanvi d'arxius per correu electrònic, per exemple utilitzant en el seu lloc sistemes específics per al tractament de les dades de clients; c) la doble verificació dels arxius abans de trametre'ls; i d) la separació de la creació i la tramesa d'arxius.

79. Aquesta violació de la seguretat afecta únicament la confidencialitat de les dades, mentre que la integritat i la disponibilitat es mantenen intactes. La violació només va afectar dues dotzenes de clients, per la qual cosa el volum de dades afectades es pot considerar baix. A més, les dades afectades no contenen dades sensibles. El fet que l'encarregat del tractament es posés immediatament en contacte amb el responsable del tractament, un cop va tenir coneixement de la violació de la seguretat de les dades, es pot considerar un factor de mitigació del risc (també cal avaluar la possibilitat que les dades s'hagin enviat a altres agents d'assegurances i, si això es confirma, cal prendre les mesures adequades). Gràcies a haver pres les mesures adequades després de la violació, és probable que no tingui cap incidència en els drets i llibertats de les persones afectades.

80. La combinació del baix nombre de persones afectades, la detecció immediata de la violació i les mesures adoptades per minimitzar-ne els efectes fan que aquest cas no comporti cap risc.

4.2.2 Cas núm. 09 - Mitigació i obligacions

81. D'altra banda, també hi intervenen altres circumstàncies d'atenuació del risc: l'agent està subjecte al deure del secret professional; va ser ell mateix qui va comunicar l'incident al responsable del tractament; i va suprimir el fitxer, quan se li va requerir. La sensibilització i, possiblement, incloure mesures addicionals a l'hora de verificar documents que continguin dades personals probablement contribuirà a evitar casos similars en el futur.

82. A més de documentar la violació de la seguretat de les dades d'acord amb el que disposa l'article 33.5, no cal adoptar cal altra mesura.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	X	X

4.3 Mesures tècniques i organitzatives per prevenir o mitigar l'impacte de les fonts internes de risc humà

83. Una combinació de les mesures que s'indiquen a continuació –aplicades d'acord amb les característiques concretes del cas– ha d'ajudar a reduir les possibilitats que es torni a produir una violació similar.

84. Mesures recomanables

(La llista de les mesures següents no es proposa com a exclusiva o completa. Al contrari, té l'objectiu d'aportar idees per a la prevenció i possibles solucions. Cada activitat de tractament és diferent i, per tant, el responsable del tractament ha de decidir quines són les mesures més adequades a la situació)

- Aplicació periòdica de programes de formació, educació i conscienciació per als empleats sobre les seves obligacions en matèria de privacitat i seguretat, així com la detecció i notificació d'amenaces per a la seguretat de les dades personals.[26] Desenvolupament d'un programa de sensibilització, per recordar als empleats els errors més comuns que ocasionen violacions de la seguretat de les dades personals i com poden evitar-les.
- Establiment de pràctiques, procediments i sistemes robustos i efectius en matèria de protecció de les dades i privacitat.[27]
- Avaluació de les pràctiques, procediments i sistemes de privacitat, per garantir-ne la continuïtat de l'eficàcia.[28]
- Aplicació de polítiques de control d'accés adequades que obliguin els usuaris a seguir les normes.
- Implantació de tècniques per forçar l'autenticació de l'usuari a l'hora d'accedir a dades personals sensibles.
- Desactivació del compte d'usuari relacionat amb l'empresa, tan bon punt aquest usuari abandona l'empresa.

[26]Secció 2, subsecció i) de la Resolució per abordar el paper de l'error humà en les violacions de la seguretat de les dades personals.
[27]Secció 2, subsecció ii) de la Resolució per abordar el paper de l'error humà en les violacions de la seguretat de les dades personals.
[28]Secció 2, subsecció iii) de la Resolució per abordar el paper de l'error humà en les violacions de la seguretat de les dades personals.

- Comprovació de fluxos de dades inusuals entre el servidor d'arxius i els equips de treball dels empleats.
- Configuració de seguretat d'interfície d'entrada i sortida en el BIOS o mitjançant l'ús de programari que controli l'ús d'interfícies informàtiques (per exemple, blocar o desblocar USB/CD/DVD, etc.).
- Revisió de la política d'accés dels empleats (com ara registrar l'accés a dades i requerir que l'usuari indiqui un motiu empresarial per accedir-hi, de manera que aquesta informació estigui disponible per a auditories).
- Desactivació dels serveis de núvol obert.
- Prohibició i impediment de l'accés a serveis de correu oberts.
- Desactivació de la funció de captura de pantalla en el sistema operatiu.
- Aplicació d'una política de taula neta.
- Bloqueig automàtic de tots els ordinadors, un cop transcorregut un determinat temps d'inactivitat.
- Ús de mecanismes per a canvis d'usuari ràpids en entorns compartits (com ara testimonis [sense fils] per obrir / iniciar sessió a comptes blocats).
- Ús de sistemes específics per gestionar dades personals que apliquin mecanismes de control d'accés i que evitin errors humans com l'enviament de comunicacions a un destinatari erroni. L'ús de fulls de càlcul i altres documents d'ofimàtica no és un mitjà adequat per gestionar les dades dels clients.

5 PÈRDUA O ROBATORI DE DISPOSITIUS I DOCUMENTS EN PAPER

85. Un tipus freqüent de cas és la pèrdua o el robatori de dispositius portàtils. En aquests casos, el responsable del tractament ha de tenir en compte les circumstàncies del tractament, com ara el tipus de dades emmagatzemades en el dispositiu, els mitjans de suport i les mesures adoptades abans de la violació per garantir un nivell de seguretat adequat. Tots aquests elements incideixen en els efectes potencials de la violació de la seguretat de les dades. Com que el dispositiu ja no està disponible, l'avaluació del risc pot resultar difícil.

86. Les violacions d'aquest tipus sempre es poden classificar com a violacions de la confidencialitat. No obstant això, si no hi ha còpia de seguretat per a la base de dades sostreta, també pot constituir una violació de la disponibilitat i de la integritat.

87. Els escenaris següents mostren de quina manera incideixen les circumstàncies esmentades anteriorment en la probabilitat i la gravetat de la violació de la seguretat de les dades personals.

5.1 Cas núm. 10: robatori de material que conté dades personals xifrades

Durant una intrusió en una llar d'infants, es van robar dues tauletes que contenien una aplicació que emmagatzemava dades personals sobre els infants que assistien al centre. Les dades afectades eren el nom, la data de naixement i dades sobre la seva educació. Tant les tauletes xifrades, que es van desconnectar en el moment del robatori, com l'aplicació estaven protegides per una contrasenya segura. El responsable del tractament tenia una còpia de seguretat de les dades disponible de manera ràpida i eficaç. Quan va tenir coneixement del robatori, poc després que es descobrís el robatori la llar d'infants va esborrar a distància totes les dades de les tauletes.

5.1.1 Cas núm. 10 - Mesures prèvies i avaluació del risc

88. En aquest cas, el responsable del tractament havia adoptat les mesures adequades per prevenir i mitigar els efectes d'una possible violació de la seguretat de les dades, xifrant el dispositiu, introduint una protecció adequada de contrasenyes i assegurant que hi hagués una còpia de seguretat de les dades emmagatzemades a les tauletes (a la secció 5.7 hi ha una llista de mesures recomanables).

89. Després de tenir coneixement de la violació, el responsable de tractament ha d'avaluar la font del risc, els sistemes en què es desenvolupa el tractament de dades, el tipus de dades personals implicades i els possibles efectes de la violació per a les persones afectades. La violació de la seguretat de les dades que s'ha descrit podria haver afectat la confidencialitat, la disponibilitat i la integritat de les dades afectades; tanmateix, gràcies als procediments adequats que el responsable del tractament va aplicar abans i després de la violació, aquests aspectes no es van veure afectats.

5.1.2 Cas núm. 10 - Mitigació i obligacions

90. La confidencialitat de les dades personals dels dispositius no es va veure compromesa, gràcies a la protecció de contrasenyes fortes implantada tant a les tauletes com a les aplicacions. Les tauletes estaven configurades de manera que l'establiment d'una contrasenya també significava que les dades del dispositiu estaven xifrades. Això es va veure reforçat per l'acció del responsable del tractament d'esborrar a distància tot el que contenien els dispositius robats.

91. Gràcies a les mesures aplicades, la confidencialitat de les dades es va mantenir intacta. A més, la còpia de seguretat garantia la disponibilitat ininterrompuda de les dades personals. Per tant, no es podia haver produït cap efecte advers.

92. Per tot això, era poc probable que la violació de la seguretat de les dades descrita comportés un risc per als drets i llibertats de les persones afectades. En conseqüència, no calia notificar-la a l'AC o a les persones afectades. Tanmateix, aquesta violació de la seguretat de les dades també s'ha de documentar d'acord amb el que disposa l'article 33.5.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones interessades
✓	X	X

5.2 Cas núm. 11: robatori de material que conté dades personals no xifrades

El bloc de notes electrònic d'un empleat d'una empresa proveïdora de serveis va ser sostret. El bloc contenia noms, cognoms, sexe, adreces i dates de naixement de més de 100.000 clients. A causa de la manca de disponibilitat del dispositiu robat, no es va poder determinar si també s'havien vist afectades altres categories de dades personals. L'accés al disc dur del bloc de notes no estava protegit per cap contrasenya. Les dades personals es van poder recuperar de les còpies de seguretat diàries disponibles.

5.2.1 Cas núm. 11 - Mesures prèvies i avaluació del risc

93. El responsable del tractament no havia adoptat mesures de seguretat prèvies, de manera que l'autor del robatori o qualsevol altra persona que tingués el dispositiu podia accedir fàcilment a les dades personals que contenia.

94. Aquesta violació de la seguretat de les dades afecta la confidencialitat de les dades emmagatzemades al dispositiu robat.

95. En aquest cas el bloc de notes amb les dades personals era vulnerable, perquè no estava protegit amb contrasenya o xifrat. L'absència de les mesures de seguretat bàsiques augmenta el nivell de risc per a les persones afectades. A més, la identificació de les persones afectades també és difícil, cosa que augmenta la gravetat de la violació de la seguretat. El nombre significatiu de persones afectades augmenta el risc. No obstant això, la violació no va afectar categories especials de dades.

96. Durant l'avaluació del risc,[29] el responsable del tractament ha de tenir en compte les possibles conseqüències i efectes adversos de la violació de la confidencialitat. Com a conseqüència de la violació de la seguretat, les persones afectades poden patir usurpació d'identitat fent ús de les dades disponibles al dispositiu robat i, per tant, es considera que el risc és alt.

5.2.2 Cas núm. 11 - Mitigació i obligacions

97. L'activació del xifratge del dispositiu i l'ús d'una contrasenya segura per protegir la base de dades emmagatzemada podria haver evitat que la violació de la seguretat de les dades comportés un risc per als drets i les llibertats de les persones afectades.

98. A causa d'aquestes circumstàncies, la notificació a l'AC és obligatòria i, a més, cal notificar-la a les persones afectades.

[29]Per obtenir informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓

5.3 Cas núm. 12: robatori d'arxius en suport paper sostrets que contenen dades sensibles

D'un centre de rehabilitació de persones drogodependents es va sostreure una llibreta en paper, que contenia dades bàsiques d'identitat i de salut dels pacients ingressats al centre. Les dades només s'emmagatzemaven en paper i no n'hi havia cap còpia de seguretat disponible per als metges que tractaven els pacients. La llibreta no estava guardada en un calaix o una sala tancats amb clau i el responsable del tractament no tenia un sistema de control d'accessos o ni cap altra mesura de seguretat per a la documentació en paper.

5.3.1 Cas núm. 12 - Mesures prèvies i avaluació del risc

99. El responsable del tractament no havia pres mesures de seguretat prèvies, de manera que la persona que trobés la llibreta podia accedir fàcilment a les dades personals que contenia. A més, la tipologia de dades personals emmagatzemades a la llibreta feia que la manca d'una còpia de seguretat de les dades constituís un factor de risc molt greu.

100. Aquest cas serveix d'exemple d'una violació de la seguretat de les dades d'alt risc. A causa de la manca de mesures de seguretat adequades, es van perdre dades de salut considerades sensibles d'acord amb l'article 9.1 de l'RGPD. Atès que es tractava d'una categoria especial de dades, els riscos potencials per a les persones afectades van augmentar, cosa que el responsable del tractament també ha de tenir en compte a l'hora d'avaluar el risc.[30]

101. Aquesta violació de la seguretat afecta la confidencialitat, la disponibilitat i la integritat de les dades personals afectades. Com a conseqüència de la violació, s'ha trencat el secret mèdic i terceres persones no autoritzades poden accedir a la informació mèdica privada dels pacients, cosa que pot tenir repercussions greus per a la vida personal dels pacients. A més, la violació de la disponibilitat pot alterar la continuïtat del tractament dels pacients. Com que no es pot descartar la modificació o supressió de parts del contingut de la llibreta, la integritat de les dades personals també està compromesa.

5.3.2 Cas núm. 12 - Mitigació i obligacions

102. A l'hora d'avaluar les mesures de protecció, també cal tenir en compte el tipus de suport on estan contingudes les dades. Com que la llibreta era un document físic, s'hauria d'haver protegit d'una manera diferent que un dispositiu electrònic. Pseudonimitzar els noms dels pacients, conservar la llibreta en un local protegit i en un calaix o una sala tancats amb clau, així com un control d'accés adequat amb autenticació per accedir-hi, podria haver evitat la violació de la seguretat de les dades.

[30] Per obtenir informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

103. La violació descrita pot afectar greument les persones afectades; per tant, és obligatori notificar-la a l'AC i comunicar-la a les persones afectades.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓

5.4 Mesures tècniques i organitzatives per evitar o mitigar els efectes de la pèrdua o robatori de dispositius

104. Una combinació de les mesures que s'indiquen a continuació –aplicades d'acord amb les característiques concretes del cas–, pot ajudar a reduir les probabilitats que es torni a produir una violació similar.

105. Mesures recomanables

(La llista de les mesures següents no és exclusiva o completa. Al contrari, l'objectiu és aportar idees de prevenció i possibles solucions. Cada activitat de tractament és diferent, per la qual cosa el responsable del tractament ha de decidir quines mesures són les més adequades a la situació.)

- Activar el xifrat del dispositiu (com ara Bitlocker, Veracrypt o DM-Crypt).
- Fer servir un codi d'accés o contrasenya a tots els dispositius. Xifrar tots els dispositius portàtils electrònics, de manera que calgui introduir una contrasenya complexa per desxifrar-los.
- Utilitzar autenticació de múltiples factors.
- Per als dispositius amb molta mobilitat, activar les funcionalitats que permeten ubicar-los en cas de pèrdua.
- Utilitzar programari o aplicacions MDM (gestió de dispositius mòbils) i la localització. Emprar filtres antireflectors. Tancar els dispositius quan no es facin servir.
- Si és possible i adequat per al tractament de dades en qüestió, desar les dades personals en un servidor final central (*back-end*), en lloc d'un dispositiu mòbil.
- Si l'equip de treball està connectat a la xarxa d'àrea local (LAN) corporativa, fer una còpia de seguretat automàtica de les carpetes de treball, sempre que sigui inevitable desar-hi dades personals.
- Utilitzar una VPN segura (per exemple, que requereixi una clau d'autenticació de segon factor separada per establir una connexió segura), per connectar dispositius mòbils a servidors *back-end*.
- Proporcionar als empleats tancaments amb clau, perquè puguin protegir físicament els dispositius mòbils que utilitzen quan no estan vigilats.
- Regular adequadament l'ús de dispositius fora de l'empresa.

- Regular adequadament l'ús de dispositius dins de l'empresa.
- Utilitzar programari o aplicacions MDM (gestió de dispositius mòbils) i activar la funció d'esborrat a distància.
- Fer servir la gestió centralitzada de dispositius, amb drets mínims per als usuaris pel que fa a instal·lar programari.
- Instal·lar controls d'accés físic.
- Evitar l'emmagatzematge d'informació sensible en dispositius o discs durs mòbils. Si cal accedir al sistema intern de l'empresa, s'han d'utilitzar canals segurs, com s'ha dit anteriorment.

6 ERROR AL CORREU POSTAL

106. En aquest cas, l'origen del risc també és un error humà intern, però no hi ha una acció malintencionada que hagi causat la violació. Ha estat fruit de la manca d'atenció. El responsable del tractament pot fer poca cosa una vegada s'ha produït; per tant, en aquests casos la prevenció encara és més important que en altres tipus de violacions.

6.1 Cas núm. 13: error al correu postal

> Una empresa minorista va empaquetar dues comandes de sabates. Per un error humà, es van barrejar dues factures. Com a resultat, tant els productes com les factures corresponents es van enviar a un destinatari erroni. Això significa que cada client va rebre la comanda de l'altre, incloses les factures amb les dades personals. Després de tenir coneixement de la violació de la seguretat de les dades, el responsable del tractament va retirar les comandes i les va enviar als destinataris correctes.

6.1.1 Cas núm. 13 - Mesures prèvies i avaluació del risc

107. Les factures contenien les dades personals necessàries per fer el lliurament correcte (nom, adreça, article comprat i preu). És important en primer lloc determinar com es va poder produir l'error humà i si, d'alguna manera, es podia haver evitat. En el cas concret descrit el risc és baix, perquè no hi estan implicades categories especials de dades o altres dades que en cas de mal ús poguessin provocar efectes negatius substancials; la violació no és conseqüència d'un error sistèmic del responsable del tractament i només afecta dues persones. No es va poder determinar cap efecte advers per als afectats.

6.1.2 Cas núm. 13 - Mitigació i obligacions

108. El responsable del tractament ha de preveure la devolució gratuïta dels articles i les factures corresponents, i sol·licitar als destinataris erronis que destrueixin o suprimeixin totes les còpies de les factures que continguin dades personals de l'altra persona.

109. Encara que la violació de la seguretat no comporta un risc alt per als drets i llibertats de les persones afectades i, per tant, la comunicació als afectats no és obligatòria d'acord amb

l'article 34 de l'RGPD, no es pot evitar comunicar-los la violació, ja que per mitigar el risc necessita la seva cooperació.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	X	X

6.2 Cas núm. 14: enviament per correu electrònic de dades personals d'alta confidencialitat per error

El departament d'ocupació d'una oficina de l'administració pública va enviar un missatge per correu electrònic a les persones inscrites com a sol·licitants d'ocupació, sobre les properes sessions formatives previstes. Per error, s'hi va adjuntar un document amb les dades personals d'aquests sol·licitants d'ocupació (nom, adreça electrònica, adreça postal i número de la seguretat social). El nombre de persones afectades supera les 60.000. Després, l'oficina es va posar en contacte amb tots els destinataris i els va demanar que eliminessin el missatge anterior i no utilitzessin la informació que contenia.

6.2.1 Cas núm. 14 - Mesures prèvies i avaluació del risc

110. S'haurien d'haver aplicat normes més estrictes per trametre aquests missatges. Cal avaluar la possibilitat d'introduir mecanismes de control addicionals.

111. El nombre de persones afectades és considerable i la implicació del seu número de la seguretat social, juntament amb altres dades personals més bàsiques, augmenta encara més el risc, que es pot considerar alt.[31] El responsable del tractament no pot evitar que qualsevol destinatari del correu divulgui les dades.

6.2.2 Cas núm. 14 - Mitigació i obligacions

112. Com ja s'ha dit, els mitjans per mitigar amb eficàcia els riscos d'una violació d'aquest tipus són limitats. Malgrat que el responsable del tractament va sol·licitar la supressió del missatge, no pot obligar els destinataris a fer-ho. En conseqüència, tampoc no pot tenir la certesa que compliran la sol·licitud.

113. En un cas com aquest, les tres accions que s'indiquen a continuació han de ser indiscutibles.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓

[31] Per obtenir informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

6.3 Cas núm. 15: enviament per correu electrònic de dades personals per error

La llista de participants en un curs d'anglès jurídic que s'ha d'impartir en un hotel durant 5 dies es va enviar per error a 15 persones que ja hi havien participat, en lloc d'enviar-se a l'hotel. La llista conté noms, adreces electròniques i preferències alimentàries dels 15 participants. Només dos dels participants han indicat les seves preferències alimentàries i han comunicat que tenen intolerància a la lactosa. Cap dels participants té una identitat protegida. El responsable del tractament s'adona de l'error immediatament després d'enviar la llista i n'informa els destinataris i els demana que suprimeixin la llista.

6.3.1 Cas núm. 15 - Mesures prèvies i avaluació del risc

114. S'haurien d'haver aplicat normes estrictes per a la tramesa de missatges que contenen dades personals. Cal avaluar la introducció de mecanismes de control addicionals.

115. Els riscos derivats de la naturalesa, la sensibilitat, el volum i el context de les dades personals són baixos. Les dades personals inclouen dades sensibles sobre les preferències alimentàries de dos dels participants. Tot i que la informació que algú és intolerant a la lactosa es considera una dada de salut, el risc que s'utilitzi de manera perjudicial s'ha de considerar relativament baix. En el cas de les dades de salut, s'acostuma a considerar que la violació pot comportar un risc alt per a la persona afectada,[32] però en aquest cas concret no es pot identificar cap risc que la violació pugui comportar danys físics, materials i immaterials per a la persona afectada, com a conseqüència de la divulgació no autoritzada d'informació sobre la intolerància a la lactosa. A diferència d'altres preferències alimentàries, normalment la intolerància a la lactosa no es pot vincular a creences religioses o filosòfiques. A més, el volum de dades afectades i el nombre de persones afectades són molt baixos.

6.3.2 Cas núm. 15 - Mitigació i obligacions

116. En resum, es pot afirmar que la violació no va tenir cap efecte significatiu per a les persones afectades. El fet que el responsable del tractament es posés en contacte immediatament amb els destinataris, quan es va assabentar de l'error, es pot considerar un factor de mitigació del risc.

117. Si s'envia un missatge de correu electrònic a un destinatari erroni o no autoritzat, es recomana que el responsable del tractament trameti un missatge de seguiment amb còpia oculta als destinataris, en què els demani disculpes i els indiqui que han d'eliminar el missatge que han rebut per error i, a més, els adverteixi que no tenen dret a fer servir les adreces electròniques que els han estat comunicades.

118. A causa d'aquests fets, era poc probable que aquesta violació de la seguretat de les dades comportés un risc per als drets i llibertats de les persones afectades. Per tant, no calia notificar-la a l'AC o a les persones afectades. Tanmateix, aquesta violació de la seguretat de les dades també s'ha de documentar d'acord amb el que disposa l'article 33.5.

[32] Vegeu les Directrius WP 250, p. 23.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	X	X

6.4 Cas núm. 16: error en el correu postal

Un grup d'assegurances ofereix assegurances per a automòbils. Per fer-ho, envia periòdicament pòlisses de cotització ajustades per correu postal. A més del nom i l'adreça del prenedor de la pòlissa, la carta conté el número de matrícula del vehicle sense ocultar, els preus de l'assegurança de l'any en curs i del següent, el quilometratge anual aproximat i la data de naixement del prenedor de la pòlissa. No s'hi inclouen dades de salut d'acord amb l'article 9 de l'RGPD, ni les dades de pagament (dades bancàries) ni dades econòmiques i financeres.

Les cartes s'ensobren mitjançant ensobradores automatitzades. A causa d'un error mecànic, es van introduir dues cartes per a dos prenedors d'assegurança diferents en el mateix sobre i es van enviar a un d'ells per correu postal. El prenedor va obrir la carta a casa seva i va examinar tant la seva carta com la de l'altre prenedor que havia rebut per error.

6.4.1 Cas núm. 16 - Mesures prèvies i avaluació del risc

119. La carta que s'ha lliurat per error conté el nom, l'adreça, la data de naixement, el número de matrícula del vehicle sense ocultar i la classificació del preu de l'assegurança de l'any en curs i de l'any següent. Els efectes per a la persona afectada s'han de considerar mitjans, ja que es comunica a una persona no autoritzada informació que no està disponible públicament, com ara la data de naixement o els números de la matrícula del vehicle, així com els increments en els preus de l'assegurança. La probabilitat d'un ús inadequat d'aquestes dades es considera entre baixa i mitjana. Tanmateix, malgrat que és probable que molts destinataris acabin llençant la carta rebuda indegudament a la paperera, no es pot descartar complement que la carta es publiqui a les xarxes socials o que es contacti amb el prenedor de la pòlissa.

6.4.2 Cas núm. 16 - Mitigació i obligacions

120. El responsable del tractament ha d'aconseguir que se li retorni el document original i s'ha de fer càrrec de les despeses de devolució. També ha d'informar la persona que va rebre la carta per error que no pot fer un ús indegut de la informació que ha llegit.

121. Probablement, mai serà possible evitar per complet un error en l'enviament postal, en un enviament massiu que utilitzi màquines totalment automatitzades. No obstant això, si la freqüència dels errors augmenta, cal comprovar si les ensobradores estan ben configurades i reben el manteniment correcte, o si hi ha altres problemes sistèmics que puguin originar la violació.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	X

6.5 Mesures tècniques i organitzatives per prevenir o mitigar els efectes dels errors en enviaments de correu

122. Una combinació de les mesures que s'indiquen a continuació –aplicades d'acord amb les característiques singulars del cas– ajudaria a reduir les probabilitats que es torni a produir una violació similar.

123. Mesures recomanables:

(La llista de les mesures següents no és exclusiva o completa. Al contrari, l'objectiu és aportar idees de prevenció i possibles solucions. Cada activitat de tractament és diferent, per la qual cosa el responsable del tractament ha de decidir quines mesures són les més adequades a la situació.)

- Establiment d'estàndards exactes, sense marge per a la interpretació, per enviar cartes i correus electrònics.
- Formació adequada per al personal sobre la manera d'enviar cartes o correus electrònics.
- Quan s'envien correus electrònics a diversos destinataris, s'han d'incloure per defecte al camp *Cco*.
- Requeriment de confirmació addicional, quan s'envien missatges a diversos destinataris que no figuren al camp *Cco*.
- Aplicació del principi que quatre ulls hi veuen més que dos.
- Introducció automàtica i no manual de les adreces electròniques, amb dades extretes d'una base de dades disponible i actualitzada; el sistema d'introducció automàtica s'ha de revisar periòdicament, per detectar errors ocults i configuracions incorrectes.
- Aplicació del retard del missatge (per exemple, el missatge es pot suprimir o modificar durant un període de temps determinat després d'haver clicat el botó d'enviar).
- Desactivació de la funció autocompletar a l'hora d'escriure les adreces electròniques.
- Sessions de conscienciació sobre els errors més comuns que originen una violació de la seguretat de les dades personals.
- Sessions de formació i manuals sobre com gestionar incidents que originen una violació de la seguretat de les dades personals i a qui cal informar-ne (implicar-hi el delegat de protecció de dades).

7 ALTRES CASOS - ENGINYERIA SOCIAL

7.1 Cas núm. 17: usurpació d'identitat

El centre de contacte d'una empresa de telecomunicacions rep una trucada telefònica d'algú que es presenta com a client. El suposat client sol·licita a l'empresa que canviï l'adreça electrònica a la qual s'han d'enviar les dades de facturació a partir de llavors. L'empleat del centre de contacte valida la identitat del client preguntant-li determinades dades personals, d'acord amb els procediments de l'empresa. La persona que ha trucat indica correctament el número d'identificació fiscal i l'adreça postal (perquè tenia accés a aquesta informació).

Després de la validació, l'operador aplica el canvi sol·licitat i, a partir d'aquell moment, la informació sobre facturació s'envia a la nova adreça electrònica. El procediment no preveu cap notificació a l'anterior adreça electrònica de contacte. El mes següent, el client legítim es posa en contacte amb l'empresa i pregunta per què no rep les factures a la seva adreça electrònica, i nega que hagi trucat per sol·licitar el canvi de l'adreça electrònica de contacte. Més tard, l'empresa s'adona que la informació s'ha enviat a un usuari il·legítim i reverteix el canvi.

7.1.1 Cas núm. 17 - Avaluació del risc, mitigació i obligacions

124. Aquest cas exemplifica la importància de les mesures prèvies. Des de la perspectiva del risc,[33] la violació presenta un nivell de risc alt, ja que les dades de facturació poden proporcionar informació sobre la vida privada de la persona afectada (com ara hàbits o contactes) i causar danys materials (per exemple, assetjament o risc per a la integritat física). Les dades personals obtingudes durant aquest atac també poden facilitar el control dels comptes d'aquesta organització o aprofitar altres mesures d'autenticació en altres organitzacions. Tenint en compte aquests riscos, la mesura d'autenticació *adequada* ha d'estar a un nivell alt, segons quines dades personals es puguin tractar com a resultat de l'autenticació.

125. En conseqüència, el responsable del tractament l'ha de notificar a l'autoritat de control i comunicar-la a la persona afectada.

126. Vist el cas, és evident que cal millorar el procés de validació del client. Els mètodes utilitzats per a l'autenticació no eren suficients. La part malintencionada es va poder fer passar per l'usuari real, mitjançant la informació disponible públicament i la informació a la qual tenia accés d'una altra manera.

127. L'ús d'aquest tipus d'autenticació estàtica basada en el coneixement (en què la resposta no canvia i la informació no és *secreta*, com ho seria amb una contrasenya) no és recomanable.

128. En lloc d'això, l'organització ha d'utilitzar una forma d'autenticació que comporti un alt grau de confiança que l'usuari autenticat és la persona real, i no una altra persona. Un mètode d'autenticació en múltiples factors amb accés fora de banda resoldria el problema. Es tractaria, per exemple, de verificar la sol·licitud de canvi enviant una petició de confirmació al contacte anterior, o afegir preguntes addicionals i demanar informació que només sigui visible a les factures anteriors. La responsabilitat de decidir quines mesures cal introduir correspon al responsable de tractament, ja que coneix millor els detalls i requisits del seu funcionament intern.

[33] Per obtenir informació sobre tractament que "comporta probablement un alt risc", vegeu la nota al peu 10.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓

7.2 Cas núm. 18: Filtració de correus electrònics

Una cadena d'hipermercats va detectar, tres mesos després de la seva configuració, que alguns comptes de correu electrònic havien estat modificats i que s'havien creat regles perquè cada correu electrònic que contingués determinades expressions (com ara *factura*, *pagament*, *transferència bancària*, *autenticació de targeta de crèdit* o *dades de compte bancari*) es traslladés a una carpeta no utilitzada i es reenviés a una adreça electrònica externa. A més, en aquell moment ja s'havia produït un atac d'enginyeria social en què l'atacant, fent-se passar per un proveïdor, havia canviat les dades bancàries d'aquest proveïdor per les seves. Finalment, en aquell moment també s'havien enviat diverses factures falses que contenien les noves dades bancàries. El sistema de monitoratge de la plataforma de correu electrònic va acabar alertant sobre les carpetes. L'empresa no va poder detectar de quina manera l'atacant va aconseguir accedir als comptes de correu electrònic per començar, però va suposar que va ser un correu electrònic infectat el responsable de donar accés al grup d'usuaris que s'ocupaven dels pagaments.

A causa del reenviament de correus electrònics basat en paraules clau, l'atacant va rebre informació sobre 99 empleats: nom i retribucions d'un mes determinat en relació amb 89 persones afectades; i nom, estat civil, nombre de fills, retribucions, jornada laboral i altra informació sobre la percepció de retribucions de 10 empleats els contractes dels quals havien finalitzat. El responsable del tractament només va notificar la violació als 10 empleats que pertanyien al segon grup.

7.2.1 Cas núm. 18 - Avaluació del risc, mitigació i obligacions

129. Encara que és probable que l'atacant no pretengués aconseguir dades personals, ja que la violació podia comportar danys tant materials (com ara pèrdues financeres) com immaterials (com ara robatori d'identitat o frau), o les dades es podien fer servir per facilitar altres atacs (per exemple, *phishing*), és probable que la violació comporti un risc alt per als drets i les llibertats de les persones físiques. Per tant, la violació s'ha de comunicar als 99 empleats i no únicament als 10 empleats dels quals es va filtrar la informació salarial.

130. Després de tenir coneixement de la violació, el responsable del tractament va forçar un canvi de contrasenya dels comptes afectats, va blocar l'enviament de missatges de correu electrònic al compte de l'atacant, va notificar l'adreça electrònica utilitzada per l'atacant al proveïdor de serveis i va millorar les alertes del sistema de vigilància, perquè emetés una alerta tan bon punt es detectés la creació d'una regla automàtica. El responsable del tractament també podia eliminar el dret dels usuaris a establir normes de reenviament, de manera que calgués sol·licitar-ho a l'equip dels serveis informàtics. També podia introduir una política en àmbits que gestionin dades financeres, per la qual un cop per setmana o més sovint els usuaris hagin de comprovar i comunicar les regles establertes als seus comptes.

131. El fet que es pugui produir una violació de la seguretat de les dades i que no es detecti durant tant de temps, i el fet que, en un termini més ampli, s'hagués pogut fer servir l'enginyeria social per alterar més dades, va posar de manifest problemes importants en el sistema de seguretat informàtica del responsable del tractament. Aquests fets s'han de resoldre sense demora, incidint en les revisions de l'automatització i els controls dels canvis i les mesures de detecció d'incidents i les mesures de resposta. Els responsables del tractament que gestionen dades sensibles, informació financera, etc. tenen més responsabilitat a l'hora de garantir una seguretat de les dades adequada.

Accions necessàries basades en els riscos identificats		
Documentació interna	Notificació a l'autoritat de control	Comunicació a les persones afectades
✓	✓	✓