DIPUTACIÓ DE VALÈNCIA

*Protecció de Dades i Seguretat de la Informació*

# Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern nº 14 | Agost 2021

## DIRECTRIUS PER A LA CORRECTA GESTIÓ DE LES BRETXES DE SEGURETAT

# Í N D E X

## DIRECTRIUS PER A LA CORRECTA GESTIÓ DE LES BRETXES DE SEGURETAT



Vos convidem a traslladar-nos les temàtiques que resulten de vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent

enllaç

*"EL REGLAMENT GENERAL DE PROTECCIÓ DE DADES (RGPD) LES FLAMA "VIOLACIONS DE SEGURETAT" I DEFINEIX PER PRODUIR-SE LA DESTRUCCIÓ, PÈRDUA O ALTERACIÓ ACCIDENTAL O IL·LÍCITA DE DADES PERSONALS TRANSMESES, CONSERVATS O TRACTATS D'UNA ALTRA FORMA, O LA COMUNICACIÓ O ACCÉS NO AUTORITZATS A AQUESTES DADES."*

## INTRODUCCIÓ

Una bretxa de seguretat és un incident de seguretat que afecta dades personals, independentment de si és la conseqüència d'un accident o d'una acció intencionada i tant si afecta dades digitals o en format paper.

El Reglament General de Protecció de Dades (RGPD) les diu "violacions de seguretat de dades personals" i defineix per produir-se la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservats o tractats d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades.

La normativa en vigor des de 2018 obliga a notificar la violació de la seguretat de les dades personals a l'autoritat de control competent tan prompte com es tinga coneixement que s'ha produït, i a tot tardar en un termini de 72 hores; llevat que puga demostrar-se, atenent la seua responsabilitat proactiva, que no existeix risc per als drets i llibertats de les persones. La Llei orgànica de Protecció de Dades i de Garanties de Drets Digitals no recull explícitament l'obligació de notificar les bretxes de seguretat a l'AEPD, ja que ja queda recollit en el RGPD, però sí que estableix que aquest incompliment és una infracció molt greu.

D'altra banda, si la bretxa poguera derivar-se un alt risc per als interessats, també caldrà comunicar-li'l a aquests, a fi que tinguen coneixement i puguen prendre sobre aquest tema les mesures oportunes.

Les violacions de seguretat o bretxes de seguretat poden afectar diferents dimensions de la seguretat:

- Confidencialitat: revelació no autoritzada o accidental de les dades personals, o el seu accés
- Integritat: una alteració no autoritzada o accidental de les dades personals
- Disponibilitat: revelació no autoritzada o accidental de les dades personals, o el seu accés.

Sobre aquests aspectes aprofundirem al llarg dels apartats següents.

***"LA DIPUTACIÓ DE VALÈNCIA COMPTE AMB UN PROCEDIMENT DE GESTIÓ D'INCIDENTS I NOTIFICACIONS DE BRETXES DE SEGURETAT QUE POT CONSULTAR-SE EN EL DEPARTAMENT DE PROTECCIÓ DE DADES I SEGURETAT DE LA INFORMACIÓ, PERÒ LES NOCIONS BÀSIQUES REFERENT A AIXÒ SÓN NECESSÀRIES EN CADASCUN DELS CENTRES GESTORS DEL TRACTAMENT DE DADES DE LA NOSTRA CORPORACIÓ."***

## POLÍTICA CORPORATIVA

Per a donar resposta als incidents amb la seguretat de la informació, hem de comptar amb els coneixements necessaris sobre la manera d'actuar. Encara que la resposta dependrà molt de la categoria d'incidència a la qual ens enfrontem, es tractarà sempre de contindre la situació evitant que el mal s'expandisca i agreuge i, posteriorment, posar remei al mateix tractant de garantir la continuïtat del servei minimitzant el risc per als drets i llibertats dels interessats. Cal recordar que podria reclamar-se responsabilitat patrimonial de l'administració pels danys i perjudicis que l'interessat haja pogut patir, llevat que la Corporació puga demostrar que ha complit fidelment amb les seues obligacions.

En aquest sentit, els articles 33 i 34 del RGPD exposen la necessitat que les organitzacions integren dins de les seues polítiques un procés de gestió de bretxes de dades personals que concrete com l'organització donarà compliment a les seues obligacions respecte a les bretxes.

Aquest procés es constitueix en una de les mesures organitzatives més importants a l'hora de salvaguardar els drets i llibertats dels interessats a través de mesures de seguretat dels tractaments. Així, és molt important que tots els usuaris de la Corporació coneguen mínimament de la gestió d'incidents i notificacions de bretxes de seguretat.

Cal assenyalar que no tindran consideració de violació o bretxa de seguretat de dades personals, a l'efecte de l'obligació de notificació a l'Autoritat de Control i comunicació als afectats, aquells incidents que:

- No afecten dades personals, és a dir, a dades que no siguen de persones físiques identificades o identificables.
- No afecten tractaments de dades personals dutes a terme en la nostra qualitat de responsable o encarregat de tractament.

D'aquesta manera, no tots els incidents de seguretat són necessàriament bretxes de dades personals i no sols els incidents que tinguen lloc sobre els tractaments automatitzats poden ser considerats bretxes de dades personals, ja que també caldria considerar els tractaments en paper.

*"EL DELEGAT DE PROTECCIÓ DE DADES ACTUA COM A PORTAVEU ÚNIC DAVANT L'AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES I SERÀ LA PERSONA QUE ATENDRÀ QUALSEVOL QÜESTIÓ, DUBTE, DRET O DENÚNCIA DELS INTERESSATS AFECTATS PER L'INCIDENT DE SEGURETAT EN QUALSEVOL DELS TRACTAMENTS DE DADES PERSONALS"*

## ROLS I RESPONSABILITATS

Depenent de si actuem com a responsable o com a encarregat del tractament, tenim imposades les unes o les altres obligacions davant l'eventualitat d'una bretxa.

### RESPONSABLE DEL TRACTAMENT

Actuant en qualitat de responsables del tractament, hem d'aplicar les mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme al RGPD:

- valoració de l'incident avaluant les conseqüències per als drets i llibertats de les persones;
- garantir que es notifica la bretxa de dades personals a l'autoritat competent, quan resulte necessari sense dilació indeguda, i també que es comunicarà la bretxa de dades personals als afectats quan siga necessari;
- comptar amb l'assessorament del Delegat de Protecció de Dades i aquest Departament de la Diputació;
- complir amb les indicacions de la Prefectura d'aquest Departament per a complir la resta d'obligacions respecte a les bretxes.

### ENCARREGAT DEL TRACTAMENT

A més de les anteriors, actuant com a encarregats del tractament tenim l'obligació de:

- informar el responsable de tractament sense dilació indeguda de les bretxes de dades personals que afecten els tractaments encarregats (aportant la informació necessària per a facilitar l'avaluació del risc), sense perjudici de les obligacions addicionals que puga haver adquirit en virtut del contracte per encàrrec de tractament;
- ajudar el responsable a garantir el compliment de les obligacions establides en el RGPD, incloent la gestió, notificació i comunicació de les bretxes de dades personals;
- executar les labors de notificació o comunicació de la bretxa que en el seu cas tinga assignades per contracte.

Assenyalar que el Delegat de Protecció de Dades actua com a portaveu únic davant l'Agència Espanyola de Protecció de Dades i serà la persona que atendrà qualsevol qüestió, dubte, dret o denúncia dels interessats afectats per l'incident de seguretat en qualsevol dels tractaments de dades personals.

*"L'AEPD ESTABLEIX UN DELS PARÀMETRES MÉS IMPORTANTS A L'HORA D'AVALUAR UNA BRETXA DE DADES PERSONALS ÉS DETERMINAR AMB EXACTITUD LA SEUA TIPOLOGIA, ÉS A DIR DETERMINAR A QUINA DIMENSIÓ/ÉS DE SEGURETAT DE LES DADES PERSONALS HA AFECTAT LA BRETXA"*

## TIPUS DE BRETXES

És impossible esperar una correcta gestió de les bretxes de seguretat si no tenim clar en quins aspectes poden manifestar-se com a tal. Més encara, la pròpia AEPD estableix que un dels paràmetres més importants a l'hora d'avaluar una bretxa de dades personals és determinar amb exactitud la seua tipologia, és a dir determinar a quina dimensió/és de seguretat de les dades personals ha afectat la bretxa.

Per això, passem a revisar els diferents tipus existents de les mateixes i alguns exemples de prevenció i/o gestió.

### CONFIDENCIALITAT

Una bretxa afecta a la confidencialitat quan les dades personals d'un tractament han pogut ser accedits per tercers sense permís, incloent quan les dades són exfiltrats. Això inclou, per exemple, els casos d'intrusió en sistema d'informació amb accés i/o exfiltració de dades personals, l'enviament de dades personals per error, la pèrdua de dispositius o documentació amb dades personals, malware de tipus ransomware amb exfiltració de dades, etc. És important saber si les dades personals afectats estaven (totalment o parcialment) xifrats de manera segura, anonimitzats o protegits de manera que siguen inintel·ligibles per a qui haja tingut accés a aquestes dades o ho puga tindre en el futur. Si és així, les conseqüències de la bretxa de confidencialitat queden en gran manera mitigades, reduint o fins i tot anul·lant els riscos derivats de l'incident.

- Exemple: bretxes causades per pèrdua o robatori de dispositius mòbils els elements d'emmagatzematge dels quals estan xifrats amb un algorisme no compromés i l'accés al dispositiu protegit per una contrasenya forta i difícilment deduïble, es pot considerar que els riscos associats a la pèrdua de confidencialitat de les dades estan apropiadament mitigats.
- Exemple: bretxes causades per la exfiltració d'un fitxer de base de dades d'usuaris contenint nom d'usuari, contrasenya, dades de contacte i adreça:
- Si les contrasenyes dels usuaris estan protegides amb un algorisme de hash considerat criptogràficament segur, de manera que són inintel·ligibles per a qui ha tingut accés a la base de dades, el risc quedaria parcialment mitigat. Si l'algorisme de hash no es considera

*"ÉS IMPORTANT DETERMINAR SI LA DISPONIBILITAT S'HA POGUT RECUPERAR O ESTÀ EN VIES DE RECUPERACIÓ, ATÉS QUE RECUPERAR LES DADES I ELS SISTEMES DE TRACTAMENT ÉS LA VIA PER A MITIGAR EL MAL."*

criptogràficament segur (md5, sha1, …) la mitigació del risc no és efectiva.

- Si el fitxer de base de dades exfiltrat estava totalment xifrat mitjançant un algorisme criptogràficament segur i la clau de xifratge no està compromesa, el risc queda mitigat de manera que en alguns casos es pot considerar que és pràcticament nul

## DISPONIBILITAT

Una bretxa afecta a la disponibilitat de les dades personals quan han estat inaccessibles de manera temporal o permanent per a qui legítimament ha de poder tractar-los o accedir a ells. Aquesta situació pot ocórrer per successos que afecten les dades personals en si mateixos o també per successos que afecten els sistemes utilitzats per al seu tractament. informar el responsable de tractament sense dilació indeguda de les bretxes de dades personals que afecten els tractaments encarregats, sense perjudici de les obligacions addicionals que puga haver adquirit en virtut del contracte per encàrrec de tractament.

És important determinar si la disponibilitat s'ha pogut recuperar o està en vies de recuperació, atés que recuperar les dades i els sistemes de tractament és la via per a mitigar el mal que poden produir aquest tipus de bretxes de dades personals.

- Exemple: bretxes causades per malware tipus ransomware en les quals es puga descartar amb certesa la exfiltració de dades i es poden restablir les dades personals i mitjans de tractament sense que afecte significativament els serveis prestats, es pot considerar que el risc s'ha mitigat adequadament. En el cas que la recuperació de les dades i/o tractaments es prolongue en el temps afectant significativament els serveis prestats, per exemple, al no existir o no funcionar sistemes de suport de dades i processos, es pot concloure que el risc no sols no ha quedat mitigat, sinó que s'està materialitzant i causant perjudicis de diversa consideració als interessats. executar les labors de notificació o comunicació de la bretxa que tinga assignades per contracte.
- Exemple: bretxes causades per malware tipus ransomware en les quals es puga descartar amb certesa la exfiltració de dades i es poden restablir les dades personals i mitjans de tractament sense que afecte significativament a

*"QUAN ES PRODUEIXEN BRETXES DE DADES PERSONALS D'INTEGRITAT, CAL DETERMINAR SI EL TRACTAMENT DE LES DADES ALTERADES IL·LEGÍTIMAMENT POT CAUSAR O HA CAUSAT ALGUN MAL ALS AFECTATS I EN EL SEU CAS SI EL MAL ES POT REVERTIR"*

els serveis prestats, es pot considerar que el risc s'ha mitigat adequadament.

- Exemple: En bretxes causades per la pèrdua o destrucció accidental de dades personals, el risc es considerarà mitigat quan existisca un pla de recuperació que incloga una còpia actualitzada i recuperable de les dades i es puga restablir la prestació del servei sense haver causat perjudicis als interessats.

## INTEGRITAT

Una bretxa afecta a la integritat quan s'han alterat les dades personals de manera il·legítima i el tractament d'aqueixes dades personals pot causar un mal als afectats.

Un dels possibles casos és que un tercer modifique en la base de dades de l'organització la informació relativa a les dades bancàries dels empleats que s'utilitzen per al pagament de les nòmines, o un alumne modifica les qualificacions en la base de dades del seu programa formatiu. Quan es produeixen bretxes de dades personals d'integritat, cal determinar si el tractament de les dades alterades il·legítimament pot causar o ha causat algun mal als afectats i en el seu cas si el mal es pot revertir.

- Exemple: Per a mitigar les bretxes d'integritat causades per la modificació de fitxers es pot implementar eines de control de la integritat dels arxius que es basen a calcular el hash de cada fitxer que es vigila i quan és modificat, encara que siga un sol bit d'algun d'aquests arxius el sistema periòdicament torna a calcular el hash de cadascun i en comparar-lo detectarà la modificació i emetrà un avís.
- Exemple: Es podrà mitigar el risc d'una bretxa d'integritat en les bases de dades comptant amb controls d'accés, alertes i registres davant modificacions. A més, implementant sistemes que auditen de manera contínua els accessos de lectura i escriptura a aquestes bases de dades.

*"PRIMER DE TOT, ÉS NECESSARI CONÉIXER QUÈ HA OCORREGUT I DE QUINA FORMA LES MESURES DE SEGURETAT HAN FUNCIONAT O PAL·LIAT ELS FETS PER A ESTABLIR SI REALMENT S'HA PRODUÏT O NO UNA VIOLACIÓ DE LA SEGURETAT DE LES DADES."*

## FASES DE GESTIÓ

Primer de tot, tal com ja s'ha referit, és necessari conéixer què ha ocorregut i de quina forma les mesures de seguretat han funcionat o pal·liat els fets per a establir si realment s'ha produït o no una violació de la seguretat de les dades.

En si, el procés de gestió i notificació d'incidents es compon de les següents fases.

### FASE 1: DETECCIÓ I ALERTA

Per tal com es conega la informació sobre l'existència d'una bretxa de seguretat, possible o confirmada, aquesta circumstància ha de comunicar-se immediatament al Delegat de Protecció de Dades.

### FASE 2: REGISTRE DE L'INCIDENT

L'incident serà registrat i anirà documentant-se el procés amb tota la informació que es vaja recopilant. La informació relativa a les decisions preses sobre la notificació a l'Autoritat de Control competent i la comunicació als afectats (inclosa una còpia de la comunicació de realitzar-se) ha de recollir-se també en aquest registre de manera detallada.

### FASE 3: ACTUACIONS DE CONTENCIÓ I RECUPERACIÓ ENFRONT DELS INCIDENTS

Enfront dels incidents de seguretat, principalment, els que afecten els sistemes d'informació automatitzats (informàtics o electrònics) es precisarà la intervenció immediata del Departament de Protecció de Dades i Seguretat de la Informació, sense perjudici d'emprendre directament algunes mesures més immediates, tot això a l'efecte de dur a terme les següents actuacions:

- **Contenció:** decisions ràpides i adopció de mesures, tècniques i organitzatives, com pot ser tancar un sistema, aïllar-lo de la xarxa, deshabilitar unes certes funcions, etc. Una vegada aplicades de les mesures, s'ha de verificar el correcte funcionament d'aquestes, confirmant la seua idoneïtat per a l'eliminació de l'incident.

- **Recuperació:** solucionat l'incident o la bretxa de seguretat, i verificada l'eficàcia de les mesures adoptades, es restablirà el servei íntegrament, confirmant el seu funcionament normal i evitant en la mesura que siga possible que succeïsquen nous incidents basats en la mateixa causa.

***"EL DELEGAT DE PROTECCIÓ DE DADES PRENDRÀ LA DECISIÓ SOBRE LA PROCEDÈNCIA O NO DE COMUNICACIÓ A L'AGÈNCIA ESPANYOLA DE PROPIETAT DE DADES. EL DPD TAMBÉ VALORARÀ SI ESCAU COMUNICAR SOBRE LA BRETXA ALS INTERESSATS AFECTATS."***

## FASE 4: VALORACIÓ DELS INCIDENTS I BRETXES DE SEGURETAT

La valoració de l'incident la realitza el Delegat de Protecció de Dades atesa la tipologia de bretxa de seguretat i una sèrie de criteris addicionals:

- Naturalesa, sensibilitat i categories de les dades personals afectats.
- Dades llegibles/il·legibles.
- Volum de dades personals.
- Facilitat d'identificació d'individus.
- Severitat de les conseqüències per als individus (si la probabilitat de la seua materialització és baixa, mitjana o alta).
- Característiques especials dels individus.
- Nombre d'individus afectats.
- Característiques de la Diputació com a responsable.
- El perfil dels usuaris afectats.
- El número i tipologia dels sistemes afectats.
- L'impacte.
- Els requeriments legals i reguladors.

A la vista dels anteriors, el Delegat de Protecció de Dades prendrà la decisió sobre la procedència o no de comunicació a l'Agència Espanyola de Propietat de Dades. En el seu cas, la comunicació inicial, amb totes les dades, es realitzarà en el termini legal o contractual, així com serà completada finalment amb informació posterior en el termini de 30 dies.

En tot cas, el DPD també valorarà si escau comunicar sobre la bretxa als interessats afectats.

## FASE 6: SEGUIMENT

Mentre no es tinga constància fefaent que la violació de dades ha sigut completament resolta i que el risc per als afectats no ha sigut eliminat o reduït a nivells de risc residual acceptable, l'assumpte de la bretxa romandrà obert, incloent perquè podran rebre's requeriments, ordres o comunicacions per part de l'AEPD.

## FASE 7: LLIÇONS APRESES

Aquesta fase té per objectiu solucionar possibles deficiències en la gestió d'incidents o incorporar millores que permeten una millor resposta en les següents execucions. Per exemple, depurar errors o actualitzar informació que s'haja evidenciat obsoleta, revisar l'eficàcia del procés de gestió i detectar nous mecanismes de control que puguen ser necessaris o millorar els ja existents.

## MATERIAL COMPLEMENTARI

- "Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el Reglament 2016/679" (Grup de Treball de l'Article 29). Consulta aquest enllaç.
- "Guidelines 01/2021 on Examples regarding Data Breach Notification" (Comité Europeu de Protecció de Dades). Consulta aquest enllaç.
- "Bretxes de seguretat: el correu electrònic i les plataformes de productivitat en línia" (AEPD). Consulta aquest enllaç..
- "Bretxes de seguretat: El Top-5 de les mesures tècniques que has de tindre en compte" (AEPD). Consulta aquest enllaç.
- "Bretxes de seguretat: comunicació als interessats" (AEPD). Consulta aquest enllaç..
- "Bretxes de seguretat: protegeix-te davant la pèrdua o robatori d'un dispositiu portàtil" (AEPD). Consulta aquest enllaç.
- "Comunica-Bretxa RGPD" (AEPD). Consulta en aquest enllaç.

## NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) publica una actualització del seu *Guia per a la notificació de bretxes de dades personals*.**
  **El document que té com a objectiu guiar als responsables dels tractaments de dades personals en la seua obligació de notificar-les a les autoritats de protecció de dades i comunicar-li-ho a les persones les dades de les quals s'hagen vist afectats.**
  Aquesta guia actualitza la versió publicada en 2018, quan va començar a aplicar-se el Reglament General de Protecció de Dades (RGPD), i inclou l'experiència recollida en aquest temps, tant a nivell nacional com en relació amb els criteris establits pel Comité Europeu de Protecció de Dades.
  Consulta la guia en aquest enllaç.

- **Una bretxa de seguretat en el sistema de certificats COVID de Madrid arribaria a deixar al descobert nombroses persones vacunades.**
  Les dades personals de milers de madrilenys, entre ells els del Rei Felip VI, el president del Govern, Pedro Sánchez, així com els d'altres càrrecs públics i personalitats haurien quedat al descobert aquest dimecres durant diverses hores a causa d'una bretxa de seguretat en els servidors de la Conselleria de Sanitat de la Comunitat de Madrid. La Conselleria ha reconegut l'existència de la bretxa, però nega que "qualsevol ciutadà" poguera accedir a la informació. No obstant això, fonts de la notícia indiquen que "amb una bretxa de seguretat d'aquest tipus, qualsevol persona amb coneixements d'informàtica pot accedir a les dades personals del sistema". Consulta la notícia en aquest enllaç.