DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 10| Abril 2021

IDENTIFICACIÓ, GESTIÓ I COMUNICACIÓ DE LES BRETXES DE SEGURETAT EN EL CONTEXT DEL RGPD

Í N D E X

IDENTIFICACIÓ, GESTIÓ I COMUNICACIÓ DE LES BRETXES DE SEGURETAT EN EL CONTEXT DEL RGPD

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

Diputació de València

Dpt. de Protecció de Dades s Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONS

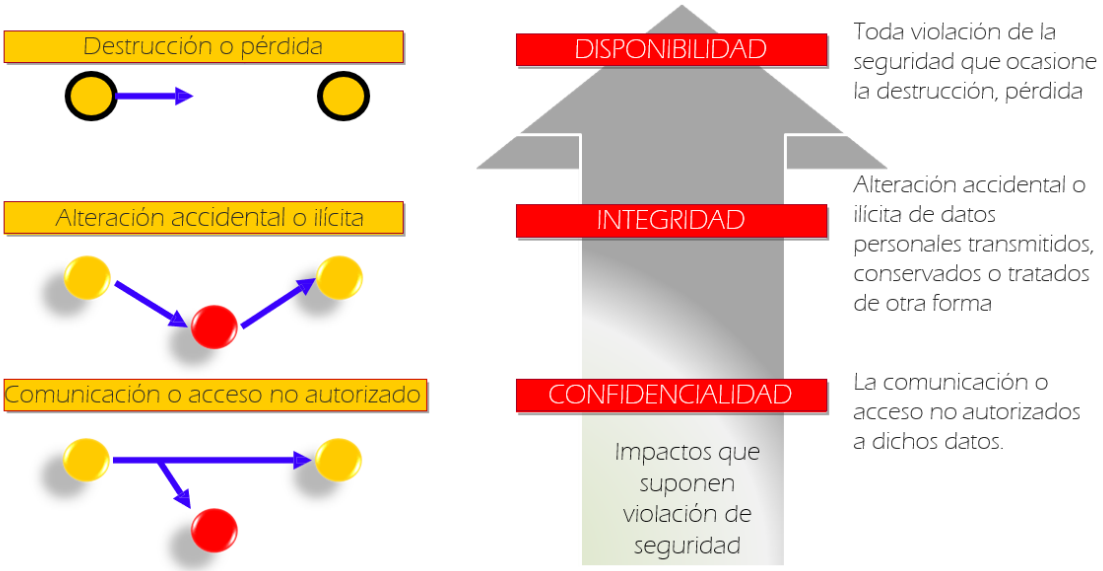
Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

Una "violació de seguretat" -també denominada "bretxa de seguretat"- és un incident de seguretat que afecta dades de caràcter personal. Aquest incident pot tindre un origen accidental o intencionat i, a més, pot afectar dades tractades digitalment o en format paper. En general, es tracta d'un succés que ocasiona la destrucció, pèrdua, alteració, comunicació o accés no autoritzat a dades personals.

El Reglament General de Protecció de Dades (RGPD) defineix les *"violacions de seguretat de les dades personals" com "totes aquelles violacions de la seguretat que ocasionen 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"*, i obliga al fet que, aquelles violacions de seguretat que puguen suposar un risc per als drets i llibertats de les persones físiques, siguen notificades a l'autoritat de control competent -en el nostre cas, es tracta de l'Agència Espanyola de Protecció de Dades (AEPD)-. En determinats casos, els de risc alt per als drets i llibertats dels interessats, s'haurà de notificar també a aquests últims.

És evident que qualsevol organització que tracte dades personals es troba exposada a patir una bretxa de seguretat que podrà repercutir en la privacitat dels interessats, per la qual cosa s'ha d'implementar un procediment per a l'adequada gestió d'aquestes. Això permetrà respondre de manera ràpida, ordenada i eficaç, minimitzant les conseqüències sobre la pròpia organització i terceres parts implicades, les quals afecten la confidencialitat, integritat o disponibilitat de les dades:



EN LA DIPUTACIÓ DE VALÈNCIA, LA GESTIÓ DE LES BRETXES DE SEGURETAT HAURÀ DE REGIR-SE PEL PROCEDIMENT INTERN VIGENT A CADA MOMENT.

IDENTIFICACIÓ

La detecció d'un incident que puga afectar la seguretat d'informació i suposar una bretxa de seguretat de les dades personals és de vital importància, ja que el RGPD estableix que s'han de notificar a l'autoritat de control competent les bretxes de seguretat que puguen suposar un risc per als drets i llibertats de les persones físiques, sense dilació indeguda i, a tot tardar, 72 hores després que s'haja tingut constància d'ella. En determinats casos, com assenyalàvem, s'haurà de notificar també als afectats, sense dilació indeguda.

Aquesta labor de detecció i identificació recaurà, en nombroses ocasions, en els usuaris dels sistemes d'informació. **Qualsevol succés que supose o poguera suposar un incident de seguretat haurà de ser comunicat immediatament per a valorar si pot catalogar-se com a "bretxa de seguretat de les dades personals".** Per exemple, hauran de comunicar-se immediatament esdeveniments com:


La pèrdua de contrasenyes d'accés als Sistemes d'Informació.


La pèrdua o robatori de suports informàtics o documents en paper amb dades de caràcter personal.


La presència d'arxius amb caràcters inusuals.


La recepció de correus electrònics amb arxius adjunts sospitosos.


El comportament estrany de dispositius.


La impossibilitat d'accedir a uns certs arxius


Atacs a la xarxa


La infecció dels sistemes d'informació per virus o altres elements nocius


La pèrdua de dades per un mal ús de les aplicacions

Els diferents moments d'atenció que requierende les bretxes de seguretat se succeeixen des de la identificació de la incidència fins al seu tancament, passant per la deguda anàlisi prèvia i, en el seu cas, respostes i/o comunicacions corresponents.

En la figura següent, extraiguda de la *Guia per a la gestió i notificació de bretxes de seguretat de l'AEPD*, podem apreciar les fases més importants en les quals podem dividir la gestió d'aquesta mena d'incidents:

La identificació d'un incident de seguretat pot produir-se a través de fonts internes a l'organització o fonts externes. Aquestes últimes serien els avisos que podem rebre de tercers (proveïdors, tècnics, etc.).

En aquest sentit, a més de complir tots els protocols de seguretat i parar atenció a les anomalies que puguen sorgir en el treball amb sistemes d'informació, cal estar pendents de les alertes que solen difondre en casos de risc els diferents organismes públics com l'Institut Nacional de Ciberseguretat (INCIBE), el Centre Criptològic Nacional (CCN), Forces i Cossos de Seguretat de l'Estat, o els mitjans de comunicació.

Una vegada identificat l'incident de seguretat, l'actuació que procedeix és una anàlisi que permeta **conéixer més detalls sobre l'incident esdevingut**, a més d'una identificació i classificació més precisa d'aquest.

A més de les respostes informàtiques reaccionàries a l'incident, és molt important que, segons quin cas, es procedisca a la notificació o comunicació de la bretxa de seguretat a l'autoritat de control. Passem a revisar-ho en els apartats següents.

"UNA VEGADA IDENTIFICAT L'INCIDENT DE SEGURETAT, EL RESPONSABLE DE SEGURETAT RECAPTARÀ MÉS DETALLS SOBRE L'INCIDENT ESDEVINGUT, PER A DECIDIR QUINES MESURES PRENDRE I PER A VALORAR LA NECESSITAT DE NOTIFICAR A L'AUTORITAT DE CONTROL I, EN EL SEU CAS, ALS AFECTATS."

ANÀLISI

EL ROL DEL DPD

Atés que el Delegat de Protecció de Dades (DPD) desenvolupa un paper molt rellevant, en aquest cas de lideratge, és important que siga consultat tan prompte s'haja detectat l'incident, la qual cosa implicarà que l'usuari que el detecte ha de comunicar-lo sense dilació. L'actuació del DPD tindrà especial rellevància en aquesta fase de comunicació perquè, entre les funcions que la normativa li atribueix, està la d'actuar com a punt de contacte entre el Responsable del tractament -la Diputació de València- i l'autoritat de control -la AEPD-.

La **informació útil al DPD** per a decidir quines mesures prendre i per a valorar la necessitat de notificar a l'autoritat de control i afectats, almenys serà la següent:

- **Mitjà pel qual s'ha materialitzat** o ha ocorregut, com per exemple: la pèrdua d'un dispositiu amb dades personals, el robatori de documentació que alberga informació de caràcter personal, la publicació de dades personals per error, l'enviament a un destinatari equivocat, un ransomware que ha xifrat un dispositiu, la intrusió no autoritzada en un sistema d'informació amb dades personals, un empleat que ha sigut víctima de phishing, etc.
- **Origen de la bretxa:** si ha sigut interna o externa i la seua intencionalitat.
- **Categories de dades:** si són dades bàsiques com a credencials o dades de contacte o si bé són categories especials, com puguen ser dades de salut.
- **Volum de dades afectades:** tant en nombre de fitxers o registres afectats com en nombre de persones les dades de les quals constaren en aquells.
- **Categories d'afectats:** empleats, ciutadans, diputats, etc. És important identificar si podria haver afectat algun col·lectiu vulnerable.
- **Informació temporal:** quan es va iniciar, quan s'ha detectat i quan ha quedat resolta.

En tot cas, cal que qualsevol bretxa de la seguretat, fets relacionats, efectes i mesures adoptades, es registre i justifique documentalment, de manera que permeta en el futur a l'autoritat de control verificar el compliment de la normativa.

COMUNICACIÓ

Amb independència de les notificacions internes que s'hagen d'efectuar per a gestionar un incident de seguretat, el RGPD estableix que, en cas de bretxa de la seguretat de les dades personals, el responsable del tractament -la Diputació de València- ha de valorar els graus de comunicació necessaris.

Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.
GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

Segons siga procedent, les comunicacions seran:

L'AUTORITAT DE CONTROL COMPETENT -AEPD-

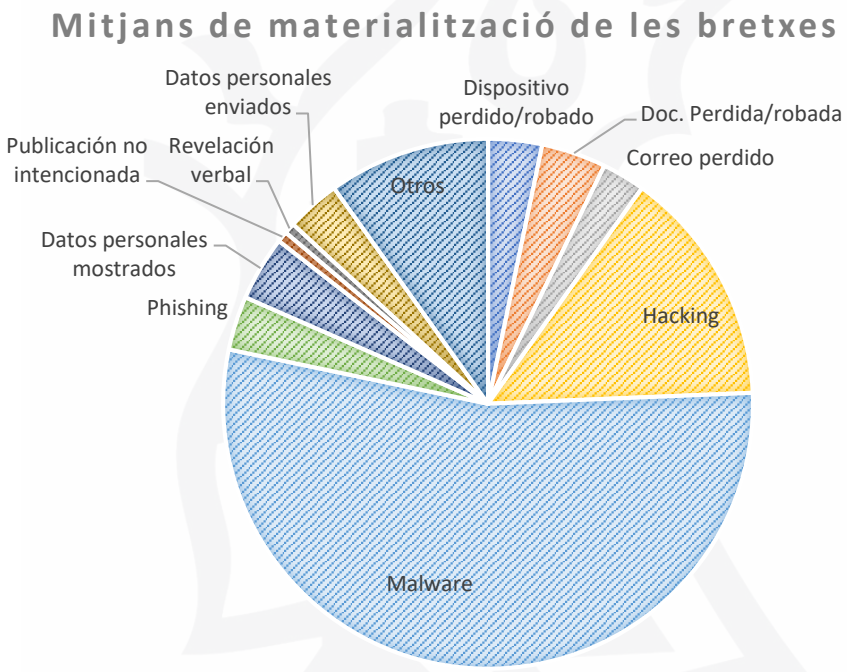
La comunicació haurà d'efectuar-se **sense dilació indeguda** i, a tot tardar, **72 hores després d'haver tingut constància d'ella**, llevat que siga improbable que aquesta bretxa de la seguretat constituïsca un **risc** per als drets i les llibertats de les persones físiques. Si en el moment de la notificació, no fora possible facilitar tota la informació, podrà facilitar-se posteriorment, de manera gradual en diferents fases. La primera notificació es realitzarà en les primeres 72h, i almenys es realitzarà una comunicació final o de tancament quan es dispose de tota la informació relativa a l'incident. La notificació a l'AEPD es realitzarà a través del formulari destinat a aquest efecte publicat en la Seu Electrònica de l'Agència**.**

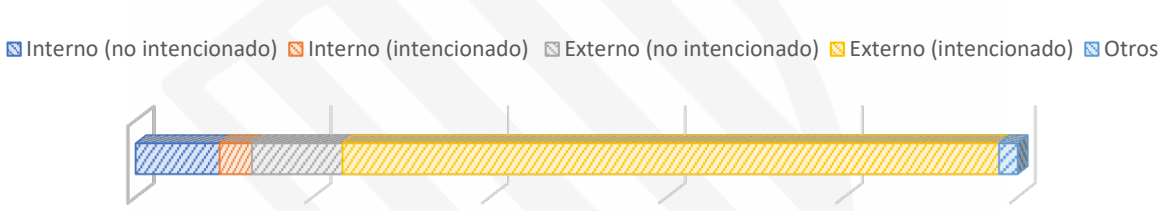
ELS AFECTATS

El RGPD també estableix els casos en els quals una bretxa de seguretat s'ha de comunicar als afectats, en concret, quan siga probable que la bretxa de la seguretat de les dades personals comporte un **alt risc** per als drets i llibertats de les persones físiques. En aquest cas, la comunicació haurà d'efectuar-se **sense dilació indeguda**. La notificació, preferentment, s'haurà de realitzar de manera directa a l'afectat, ja siga per telèfon, correu electrònic, SMS, a través de correu postal, o a través de qualsevol altre mig dirigit a l'afectat que es considere adequa.

TENDÈNCIES ACTUALS

L'Agència Espanyola de Protecció de Dades (AEPD) publica, mensualment, un informe que resumeix les característiques principals de les notificacions de bretxes de seguretat rebudes. En el seu últim informe, publicat el mes de març, s'assenyala que durant el mes de febrer es va experimentar un **increment substancial en les notificacions rebudes** respecte al mes anterior, a causa d'un incident de seguretat de tipus ransomware en un encarregat de tractament. L'informe recull les notificacions de bretxes de seguretat de les dades personals rebudes durant febrer de 2021, sent un total de **146 notificacions**. El mes de gener, el nombre de bretxes notificades a l'AEPD va ser de 88.





AL FEBRER DE 2021, L'AEPD VA REBRE 146 NOTIFICACIONS DE BRETXES DE SEGURETAT, UN NÚMERO SUBSTANCIALMENT SUPERIOR A les NOTIFICADES AL GENER (88). LA MAJORIA DE BRETXES VAN SER PROVOCADES, DE MANERA INTENCIONADA, PER UN AGENT EXTERN A les ORGANITZACIONS, SENT EL MALWARE EL MITJÀ DE MATERIALITZACIÓ MÉS HABITUAL

MATERIAL COMPLEMENTARI

- Web de l'Agència Espanyola de Protecció de Dades (AEPD). Apartat dedicat a "Bretxes de seguretat". Consulta aquest enllaç.
- Directrius sobre la notificació de les violacions de la seguretat de les dades personals d'acord amb el RGPD (Grup de Treball de l'Article 29). Consulta aquest enllaç.
- Guia per a la gestió i notificació de bretxes de seguretat (AEPD). Consulta aquest enllaç.
- Formulari de notificació de bretxes de seguretat de la Seu Electrònica (AEPD). Consulta aquest enllaç.
- Bretxes de seguretat de dades personals: què són i com actuar (Blog AEPD). Consulta aquest enllaç.
- Bretxes de seguretat: el correu electrònic i les plataformes de productivitat en línia (Blog AEPD). Consulta aquest enllaç.
- Bretxes de seguretat: El Top 5 de les mesures tècniques a tindre en compte (Blog AEPD). Consulta aquest enllaç.
- Bretxes de seguretat: comunicació als interessats (Blog AEPD). Consulta aquest enllaç.
- Bretxes de seguretat: protegeix-te davant el ransomware. Consulta aquest enllaç.

NOTÍCIES

- **El recent ciberatac contra el Servei d'Ocupació Pública Estatal (SEPE) ha posat de manifest les vulnerabilitats a les quals s'enfronten diàriament els organismes de l'Estat davant les amenaces cibernètiques.**

  El nombre de ciberatacs amb 'ransomware' a Espanya va créixer un 160% en l'últim trimestre de 2020. No obstant això, l'administració pública espanyola no és més vulnerable que la dels països del nostre entorn europeu. Continuar llegint a través d'aquest enllaç.

- **Les bretxes de seguretat també ocorren en les companyies tecnològiques més grans del món.**

  Arxius amb dades personals de 533 milions d'usuaris de Facebook van aparéixer en un xicotet fòrum de hacking. Les dades inclouen el número de telèfon, nom complet, número d'identificació en Facebook, localització actual i anterior, data de naixement, correu electrònic, data de creació, estat sentimental i biografia. La particularitat de la bretxa és que inclou centenars de milions de números de telèfon vinculats als seus propietaris, entre ells 10,8 milions d'espanyols i d'altres països llatinoamericans. Facebook diu que les dades pertanyen a una bretxa posada pegats en 2019, amb el que la informació filtrada té almenys un parell d'anys. Consulta la notícia en aquest enllaç.

- **Hackean milers de càmeres de seguretat: accedeixen a presons, hospitals i a fàbriques de Tesla.**

  Al març han sigut afectades més de 150.000 cambres, a les quals els hackers han tingut accés degut a una bretxa de seguretat. Consulta la notícia en aquest enllaç.