



Junta de Andalucía



Consejo de Transparencia  
y Protección de Datos  
de Andalucía

---

## INFORME ANUAL BRECHAS SEGURIDAD DATOS PERSONALES 2023

---





## 1. DESTACADO

La **gestión adecuada de las brechas de seguridad de datos personales** como incidentes de seguridad que pueden ocasionar la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos, es esencial para salvaguardar los derechos y libertades de las personas físicas, concretamente el derecho fundamental a la privacidad y a la protección de los datos personales.

El RGPD<sup>1</sup> impone a los responsables del tratamiento la **obligación de notificar las brechas** a las autoridades de control competentes (art.33 RGPD) y en situaciones que puedan suponer alto riesgo, **comunicarlas a los interesados** afectados (art.34 RGPD). Esta obligación tiene como objetivo garantizar que las **brechas se aborden de una manera diligente y con transparencia**, que se tomen las **medidas correctivas adecuadas** para proteger los derechos de las personas afectadas y **minimizar cualquier daño potencial** a las mismas. El conocimiento, en su caso, de las existencia de la brecha, permitirá también actuar a dichas personas en la defensa de sus intereses.

Las **notificaciones de brechas de datos personales** pueden notificarse al Consejo a través de la [Ventanilla Electrónica](#).

Del **análisis de las brechas** de seguridad de datos personales notificadas al Consejo durante el año 2023, destacan las **siguientes conclusiones**:

- Las causas más frecuentes de brechas son el ciberataque y la pérdida o robo de dispositivos, siendo necesario **reforzar la seguridad tanto lógica como física de la infraestructura y dispositivos físicos**. La mayoría de las brechas podrían haberse **evitado implantando medidas de seguridad básicas**.
- En algunos casos, se **gestionan las brechas solo de manera formal**, sin investigar sus causas ni como evitar que vuelvan a producirse. Se recomienda a los organismos la **revisión del procedimiento** de gestión de brechas de datos personales, a fin de dotarlo de **mayor agilidad, seguimiento y coordinación** de las acciones realizadas.
- Se detecta **cierta resistencia de los organismos** afectados a comunicar a los interesados las brechas que pueden suponer un alto riesgo para los mismos. Se recomienda a los organismos **mejorar el procedimiento de toma de decisión de comunicación** de brechas de seguridad a los interesados, **particularmente el análisis de riesgos derivados de la misma**, para **actuar sin dilación indebida**.

1 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).



El Consejo ha elaborado unas [Orientaciones para comunicación a afectados por brechas de datos personales](#) para facilitar dicha acción a los responsables y puede obtenerse **más información** sobre cómo notificar y gestionar una brecha en la [página web del Consejo](#).

- Es frecuente la **falta de detalle** en elementos clave de la descripción de la brecha que se notifica al Consejo, tales como:
  - tipologías de **datos y de personas afectados**, así como su número;
  - **análisis de las posibles consecuencias de la brecha**, en concreto determinar exfiltraciones
  - descripción de las **medidas correctivas adoptadas o propuestas**

Se recomienda realizar un **mayor esfuerzo en la cumplimentación** de los informes sobre las brechas, atendiendo al menos al **contenido mínimo establecido en el artículo 33.3 RGPD**.

- En el año 2023 el número de **notificaciones de brechas se ha incrementado un 26%** respecto al número registrado en el año 2022.

Con carácter general, se recuerda que los **organismos deben incluir en sus políticas de seguridad la obligación de notificar las brechas de seguridad** de los datos personales y controlar su cumplimiento.



## 2. DETALLE DE NOTIFICACIONES

En este informe se resumen las características principales de las notificaciones de brechas de datos personales notificadas al Consejo en virtud del artículo 33 del RGPD.

El informe recoge las notificaciones de brechas de datos personales recibidas durante el año 2023 en el Consejo de Transparencia y Protección de datos de Andalucía

<b>PROVINCIA</b>	
ALMERÍA	<b>4</b>
CÁDIZ	<b>4</b>
CÓRDOBA	<b>5</b>
GRANADA	<b>6</b>
HUELVA	<b>4</b>
JAÉN	<b>2</b>
MÁLAGA	<b>7</b>
SEVILLA	<b>16</b>
<b>TOTAL .....</b>	<b>48</b>

<b>TIPO ENTIDAD</b>	
ADMINISTRACIÓN AUTONÓMICA	<b>16</b>
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. AUTONÓMICA	<b>5</b>
ADMINISTRACIÓN LOCAL	<b>16</b>
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. LOCAL	<b>3</b>
No es de competencia del CTPDA	<b>3</b>
OTROS	<b>0</b>
SISTEMA UNIVERSITARIO ANDALUZ	<b>5</b>
<b>TOTAL .....</b>	<b>48</b>



<b>CONTEXTO</b>	
INTERNO (acción NO intencionada)	15
INTERNO (acción intencionada)	5
EXTERNO (acción NO intencionada)	4
EXTERNO (acción intencionada)	24
<b>TOTAL .....</b>	<b>48</b>

<b>DIMENSIÓN AFECTADA</b>	
CONFIDENCIALIDAD	<b>52</b>
INTEGRIDAD	<b>10</b>
DISPONIBILIDAD	<b>15</b>

<b>PERSONA QUE NOTIFICA</b>	
HOMBRE	<b>29</b>
MUJER	<b>19</b>
ENTIDAD / NO CONSTA	<b>0</b>
<b>TOTAL .....</b>	<b>48</b>

<b>MOTIVO PRINCIPAL</b>	
ERROR	<b>4</b>
DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD	<b>17</b>
ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE	<b>26</b>
INCIDENCIA TÉCNICA	<b>1</b>
<b>TOTAL .....</b>	<b>48</b>



<b>TIPO INCIDENTE</b>	
ABUSO DE PRIVILEGIOS DE ACCESO	<b>4</b>
ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO	<b>1</b>
PUBLICACIÓN INDEBIDA	<b>3</b>
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	<b>6</b>
REVELACIÓN INDEBIDA DE DATOS PERSONALES	<b>4</b>
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	<b>12</b>
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O EN LOCALIZACIÓN INSEGURA O ELIMINADA INCORRECTAMENTE	<b>5</b>
CIBERINCIDENTE: HACKING, MALWARE O PHISHING	<b>13</b>
<b>TOTAL .....</b>	<b>48</b>

<b>SEVERIDAD</b>	
BAJA	<b>36</b>
MEDIA	<b>3</b>
ALTA	<b>9</b>
<b>TOTAL .....</b>	<b>48</b>

<b>COMUNICACIÓN AFECTADOS</b>	
SÍ	<b>15</b>
NO SE VA A COMUNICAR	<b>17</b>
NO, PERO SE COMUNICARÁ	<b>5</b>
PDTE. DECISIÓN	<b>11</b>
NO CONSTA	<b>0</b>
<b>TOTAL .....</b>	<b>48</b>



<b>CATEGORÍAS DATOS ESPECIALES (S/N)</b>	
SÍ	15
NO	33
<b>TOTAL .....</b>	<b>48</b>

<b>SITUACIÓN</b>	
PTE. ACUSE	<b>0</b>
PTE. ANÁLISIS	<b>0</b>
PTE. MÁS DOC.	<b>4</b>
PTE. DECISIÓN	<b>0</b>
ARCHIVADA	<b>40</b>
EXPTE. POSIBLE INFRACCIÓN	<b>0</b>
CIERRE POR TRASLADO A INSPECCIÓN	<b>4</b>
<b>TOTAL .....</b>	<b>48</b>

<b>HISTÓRICO DE BRECHAS</b>	<b>AÑO</b>					<b>TOTAL</b>
	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	
<b>SITUACIÓN</b>						
PTE. ACUSE	0	0	0	0	0	<b>0</b>
PTE. ANÁLISIS	0	0	0	0	0	<b>0</b>
PTE. MÁS DOC.	0	0	0	0	4	<b>4</b>
PTE. DECISIÓN	0	0	0	0	0	<b>0</b>
ARCHIVADA	5	22	36	34	40	<b>137</b>
EXPTE. POSIBLE INFRACCIÓN	0	0	0	0	0	<b>0</b>
CIERRE POR TRASLADO A INSPECCIÓN	0	0	0	4	4	<b>8</b>
<b>TOTAL .....</b>	<b>5</b>	<b>22</b>	<b>36</b>	<b>38</b>	<b>48</b>	<b>149</b>