Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

# INFORME BRECHAS SEGURIDAD DATOS PERSONALES

## PRIMER SEMESTRE 2026

C/ Conde de Ibarra, 18. 41004. protecciondedatos.ctpda@juntadeandalucia.es

## 1. GESTIÓN DE LAS BRECHAS DE SEGURIDAD DE DATOS PERSONALES

La gestión de una brecha de datos personales comprende varias actuaciones relacionadas, pero diferentes: detectar y contener el incidente, evaluar y documentar sus consecuencias, notificarlo a la autoridad de control y, cuando pueda entrañar un alto riesgo, comunicarlo a las personas afectadas.

El responsable debe notificar la brecha al Consejo sin dilación indebida y, de ser posible, dentro de las 72 horas siguientes a haber tenido constancia de ella, salvo que resulte improbable que entrañe un riesgo para los derechos y libertades de las personas. La falta de información completa no justifica retrasar la notificación. La información disponible puede facilitarse inicialmente y completarse de forma gradual. Y en cualquier caso, todas las brechas deben quedar documentadas, incluidas las razones que justifican la decisión de notificarlas o no.

Debe destacarse que la notificación no constituye por sí misma un indicio de incumplimiento. Forma parte de la gestión responsable del incidente y permite a la autoridad de control valorar sus consecuencias, supervisar la respuesta y, cuando resulte necesario, impulsar medidas adicionales de protección.

## 2. PRINCIPALES RESULTADOS DEL SEMESTRE

Durante el primer semestre de 2026 se recibieron 32 notificaciones, una cifra reducida atendiendo a la amplitud del ámbito competencial del Consejo y al volumen y diversidad de los tratamientos realizados. Aunque este dato no permite conocer el número real de brechas producidas, resulta razonable considerar que una parte de ellas no está siendo detectada o notificada.

Todas las brechas afectaron a la confidencialidad de los datos y dos incidieron también en su disponibilidad. La mayor parte fueron calificadas como de severidad baja (26 de las 32), cinco como de severidad media y una como alta.

En las notificaciones que incorporaron información cuantitativa se contabilizaron, al menos, 98.877 personas afectadas, pero el impacto se concentró en pocos incidentes: las cinco brechas que afectaron a más de 1.000 personas reunieron aproximadamente el 97,6 % del total comunicado.

Estos datos muestran que el número de notificaciones no refleja por sí solo su impacto. Una sola brecha puede afectar a varias entidades y a un número elevado de personas, especialmente cuando se produce en un proveedor o subencargado que presta servicios a distintos responsables.

Las causas se distribuyen de forma relativamente equilibrada. Trece brechas tuvieron como motivo principal un error y doce estuvieron relacionadas con ataques, pérdidas, robos o ciberincidentes. Además, 19 se produjeron en un contexto interno no intencionado y 11 tuvieron su origen en una actuación externa intencionada.

La prevención debe atender, por tanto, tanto a los ataques externos como a los errores producidos durante la gestión ordinaria de expedientes, comunicaciones y publicaciones.

## 3. PRINCIPALES ÁMBITOS DE MEJORA

### 3.1. Detección y trazabilidad

En algunos incidentes relevantes, la detección se produjo como consecuencia de avisos externos. También se han observado dificultades para determinar el alcance de la brecha por no disponer de registros suficientes sobre los accesos y operaciones realizados.

Estas circunstancias muestran la importancia de disponer de mecanismos propios de detección, monitorización y respuesta. Las entidades deben poder determinar qué sistemas y datos se han visto afectados, durante cuánto tiempo y con qué posibles consecuencias. Para ello, necesitan registros adecuados, procedimientos de conservación de evidencias y capacidad para analizar el incidente.

La falta de detalle en una notificación no siempre responde a una cumplimentación insuficiente del formulario. También puede revelar que la entidad no dispone de la trazabilidad necesaria para reconstruir lo sucedido. Esta carencia dificulta la evaluación del riesgo, la comunicación a las personas afectadas y la adopción de medidas correctivas.

### 3.2. Prevención de errores

El tipo de incidente más frecuente en el semestre fue el envío o exposición de datos a destinatarios incorrectos. A ello se añaden supuestos de publicación indebida, uso incorrecto del correo electrónico y tratamiento inseguro de documentación.

La formación y concienciación del personal siguen siendo necesarias, pero no deben constituir la única medida preventiva. Cuando el error sea razonablemente previsible, los procedimientos y sistemas deben incorporar controles que reduzcan la posibilidad de que se produzca.

Entre estos controles se encuentran la verificación de destinatarios y documentos adjuntos, la revisión previa de las publicaciones, la configuración restrictiva de permisos y la comprobación de la información antes de su puesta a disposición.

La respuesta tampoco debe limitarse únicamente a retirar la información o solicitar su eliminación. Debe analizarse la causa del error y determinarse si procede modificar el procedimiento, el sistema o la distribución de responsabilidades.

### 3.3. Seguridad y minimización desde el diseño

Las brechas analizadas muestran la necesidad de mantener una gestión continuada de la seguridad. La existencia de sistemas desactualizados, vulnerabilidades no corregidas, registros insuficientes o información accesible desde entornos no adecuadamente protegidos puede ampliar considerablemente el alcance de un incidente.

Las entidades deben aplicar las medidas correspondientes del Esquema Nacional de Seguridad y las exigencias del artículo 32 RGPD. Estas medidas deben incluir la actualización de los sistemas, la gestión de vulnerabilidades, el control de accesos, la protección de las copias de seguridad y la capacidad de detectar accesos no autorizados.

La seguridad también exige reducir la información que puede quedar expuesta. La recogida o conservación de documentación identificativa, información económica u otros datos de riesgo elevado puede incrementar las posibles consecuencias de una brecha.

La minimización y la limitación del plazo de conservación constituyen, por tanto, medidas de seguridad material. Las entidades deben revisar qué datos necesitan y durante cuánto tiempo deben conservarlos.

### 3.4. Responsabilidad sobre usuarios y proveedores

En la gestión de los tratamientos es habitual que intervengan proveedores, subencargados y diferentes unidades o personas usuarias de los sistemas. Esta intervención no elimina la responsabilidad de la entidad sobre los tratamientos que dirige.

Los responsables deben mantener una capacidad efectiva de supervisión sobre toda la cadena del tratamiento. Esto exige delimitar las funciones, establecer canales de comunicación inmediata de incidentes, controlar la intervención de subencargados y comprobar la implantación de las medidas de seguridad comprometidas.

Tampoco resulta adecuado atribuir a los usuarios individuales la administración y actualización de sistemas que tratan datos personales. La entidad debe establecer un marco de gobierno que permita conocer los sistemas existentes, controlar su actualización, detectar vulnerabilidades y retirar o aislar aquellos que no cumplan las condiciones de seguridad exigibles.

## 4. COMUNICACIÓN A LAS PERSONAS AFECTADAS

La comunicación consta realizada en 20 de las 32 brechas notificadas, frente a 11 de las 29 registradas durante el primer semestre de 2025. Un aumento significativo. No obstante, este dato debe interpretarse con prudencia, porque la comunicación solo resulta obligatoria cuando sea probable que la brecha entrañe un alto riesgo.

Su adecuación al RGPD tampoco depende únicamente de que se haya efectuado. Una comunicación incompleta o excesivamente genérica puede impedir que las personas comprendan el riesgo y adopten las medidas de protección necesarias.

La comunicación debe describir de manera clara la naturaleza de la brecha, los datos comprometidos, las posibles consecuencias, las medidas adoptadas y las actuaciones que pueden realizar las personas afectadas. Su finalidad no es únicamente informar de que se ha producido un incidente, sino permitir una respuesta efectiva frente al fraude, la suplantación de identidad, la reutilización de credenciales u otros daños previsibles.

Cuando exista alto riesgo, la comunicación debe efectuarse sin dilación indebida. No debe demorarse hasta que concluya íntegramente el análisis técnico si ya se dispone de información suficiente para advertir a las personas afectadas. Puede realizarse una primera comunicación con la información disponible y completarse posteriormente.

En cualquier caso, la decisión de comunicar o no debe quedar motivada y documentada.

## 5. MEDIDAS CORRECTIVAS Y APRENDIZAJE

La gestión de una brecha no finaliza con su notificación ni con la contención inmediata. Deben identificarse sus causas y adoptarse medidas que reduzcan la posibilidad de repetición.

Durante el semestre se han observado respuestas adecuadas y proporcionadas, como la retirada preventiva de servicios, la realización de análisis especializados, la revisión de procedimientos y la comprobación de la seguridad antes de restablecer los sistemas.

No obstante, debe distinguirse entre medidas previstas y medidas efectivamente implantadas. El responsable debe comprobar y documentar su ejecución y eficacia. Cuando intervengan encargados o subencargados, también debe supervisar que las medidas comprometidas hayan sido desplegadas por estos.

En conjunto, las brechas notificadas permiten extraer una conclusión general positiva sobre las entidades. La mayoría presentaron una severidad baja y en numerosos casos se adoptaron medidas de contención, comunicación y revisión ágiles y diligentes. Sin embargo, algunos

incidentes concentraron un impacto elevado y pusieron de manifiesto ámbitos de mejora relacionados con la detección, la trazabilidad, el gobierno de los sistemas, la minimización y la comunicación a las personas afectadas.

El Consejo dispone de una Ventanilla Electrónica para la notificación de brechas y de unas Orientaciones para la comunicación a las personas afectadas.

## 6. 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 primer semestre del año 2026 en el Consejo de Transparencia y Protección de datos de Andalucía.

| PROVINCIA | |
|---|---|
| ALMERÍA | 0 |
| CÁDIZ | 5 |
| CÓRDOBA | 3 |
| GRANADA | 2 |
| HUELVA | 2 |
| JAÉN | 4 |
| MÁLAGA | 1 |
| SEVILLA | 15 |
| TOTAL ..... | 32 |

| TIPO ENTIDAD | |
|---|---|
| ADMINISTRACIÓN AUTONÓMICA | 11 |
| ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. AUTONÓMICA | 2 |
| ADMINISTRACIÓN LOCAL | 10 |
| ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. LOCAL | 2 |
| SISTEMA UNIVERSITARIO ANDALUZ | 4 |
| OTROS (tales como instituciones del Parlamento de Andalucía, colegios profesionales) | 3 |
| TOTAL ..... | 32 |

| CONTEXTO | |
|---|---|
| INTERNO (acción NO intencionada) | 19 |
| INTERNO (acción intencionada) | 1 |
| EXTERNO (acción NO intencionada) | 1 |
| EXTERNO (acción intencionada) | 11 |
| TOTAL ..... | 32 |

| DIMENSIÓN AFECTADA * | |
|---|---|
| CONFIDENCIALIDAD | 32 |
| INTEGRIDAD | 0 |
| DISPONIBILIDAD | 2 |

* una misma brecha puede afectar a varias dimensiones

| MOTIVO PRINCIPAL | |
|---|---|
| ERROR | 13 |
| DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD | 2 |
| ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE | 12 |
| INCIDENCIA TÉCNICA | 5 |
| TOTAL ..... | 32 |

| TIPO INCIDENTE | |
|---|---|
| INCIDENCIA TÉCNICA | 2 |
| DATOS PERSONALES MODIFICADOS/PERDIDOS/BORRADOS | 0 |
| ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO | 1 |
| PUBLICACIÓN INDEBIDA | 2 |
| DATOS ENVIADOS /MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE) | 14 |
| REVELACIÓN INDEBIDA DE DATOS PERSONALES | 0 |
| DISPOSITIVO PERDIDO, ROBADO O DESECHADO | 1 |
| DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O UBICACIÓN INSEGURA O EXTRAVIADA EN ENTREGA POSTAL O ELIMINADA INDEBIDAMENTE | 1 |
| CIBERINCIDENTES: HACKING, MALWARE, RANSOMWARE, PHISHING | 11 |
| TOTAL ..... | 32 |

| SEVERIDAD | |
|---|---|
| BAJA | 26 |
| MEDIA | 5 |
| ALTA | 1 |
| TOTAL ..... | 32 |

| COMUNICACIÓN AFECTADOS POR RESP.TTO | |
|---|---|
| SÍ | 20 |
| NO SE VA A COMUNICAR | 3 |
| NO, PERO SE COMUNICARÁ | 3 |
| PDTE. DECISIÓN POR PARTE DE RESP. TRATAMIENTO | 4 |
| NO CONSTA | 2 |
| TOTAL ..... | 32 |

| CATEGORÍAS DATOS ESPECIALES | |
|---|---|
| SÍ | 5 |
| NO | 27 |
| TOTAL ..... | 32 |

| GÉNERO PERSONA QUE NOTIFICA | |
|---|---|
| HOMBRE | 21 |
| MUJER | 11 |
| ENTIDAD / NO CONSTA | 0 |
| TOTAL ..... | 32 |

| NÚMERO DE CIUDADANOS AFECTADOS | brechas | afectados |
|---|---|---|
| 1 | **11** | **11** |
| 2-10 | **5** | **21** |
| 11-100 | **3** | **254** |
| 101-1000 | **6** | **2.118** |
| 1001-10000 | **4** | **18.629** |
| MÁS DE 10000 | **1** | **77.844** |
| NÚMERO NO INDICADO | **2** | |
| **TOTAL .....** | **32** | **98.877** |