



Junta de Andalucía



Consejo de Transparencia
y Protección de Datos
de Andalucía

**INFORME BRECHAS SEGURIDAD DATOS PERSONALES
PRIMER SEMESTRE 2024**





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 RGPD¹ impone a los responsables del tratamiento la **obligación de notificar las brechas** a las autoridades de control competentes, salvo que sea improbable que conlleven un riesgo (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** al Consejo pueden realizarse a través de la [Ventanilla Electrónica](#) y puede obtenerse más información sobre cómo notificar y gestionar una brecha en la [página web del Consejo](#).

Por otra parte, pueden consultarse las [Orientaciones para comunicación a afectados por brechas de datos personales](#) elaboradas por este Consejo.

Del **análisis de las brechas** de seguridad de datos personales notificadas al Consejo durante el primer semestre del año 2024, destacan las **siguientes conclusiones**:

- Las causas más frecuentes de brechas son el ciberataque y los errores en los envíos de correos electrónicos, por lo que conviene observar las siguientes recomendaciones:
 - **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**.
 - **desplegar procedimientos que verifiquen la corrección de los envíos por email** o incluso correo postal, así como una **mayor concienciación del personal** en este aspecto, extremando las precauciones en los casos que se traten datos sensibles.
- **Aumentan las comunicaciones a los afectados**, siendo no obstante, aún prematuro extraer conclusiones al respecto.

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).



- Se dan casos en los que **las brechas se gestionan 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.
- Es frecuente la **falta de detalle** en elementos clave de la descripción de la brecha que se notifica al Consejo, tales como:
 - el número de afectados. Aunque sea estimado, es esencial para determinar el **impacto colectivo de las brechas**.
 - tipologías de **datos (en particular, datos sensibles) y de personas afectadas**,
 - 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**.

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 primer semestre del año 2024 en el Consejo de Transparencia y Protección de datos de Andalucía.

PROVINCIA	
ALMERÍA	0
CÁDIZ	1
CÓRDOBA	3
GRANADA	0
HUELVA	2
JAÉN	0
MÁLAGA	6
SEVILLA	9
TOTAL	21

TIPO ENTIDAD	
ADMINISTRACIÓN AUTONÓMICA	6
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. AUTONÓMICA	4
ADMINISTRACIÓN LOCAL	5
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. LOCAL	5
SISTEMA UNIVERSITARIO ANDALUZ	1
TOTAL	21

INTERNO (acción NO intencionada)	11
INTERNO (acción intencionada)	1
EXTERNO (acción NO intencionada)	3
EXTERNO (acción intencionada)	6
TOTAL	21



DIMENSIÓN AFECTADA	
CONFIDENCIALIDAD	18
INTEGRIDAD	1
DISPONIBILIDAD	6

PERSONA QUE NOTIFICA	
HOMBRE	8
MUJER	13
ENTIDAD / NO CONSTA	0
TOTAL	21

MOTIVO PRINCIPAL	
NO COMPETE CTYPDA	0
ERROR	7
DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD	4
ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE	9
INCIDENCIA TÉCNICA	1
TOTAL	21

TIPO INCIDENTE	
NO COMPETE CTYPDA	0
INCIDENCIA TÉCNICA	1
DATOS PERSONALES MODIFICADOS / PERDIDOS / BORRADOS	0
ABUSO DE PRIVILEGIOS DE ACCESO	0
ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO	0
PUBLICACIÓN INDEBIDA	3
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	5
REVELACIÓN INDEBIDA DE DATOS PERSONALES	1
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	1
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O EN LOCALIZACIÓN INSEGURA O ELIMINADA INCORRECTAMENTE	4
CIBERINCIDENTE: HACKING, MALWARE O PHISHING	6
TOTAL	21



SEVERIDAD	
BAJA	14
MEDIA	6
ALTA	1
TOTAL	21

COMUNICACIÓN AFECTADOS	
SI	11
NO SE VA A COMUNICAR	1
NO, PERO SE COMUNICARÁ	3
PDTE. DECISIÓN	6
NO CONSTA	0
TOTAL	21

CATEGORÍAS ESPECIALES (S/N)	
SÍ	6
NO	15
TOTAL	21

SITUACIÓN	
PTE. ACUSE	0
PTE. ANÁLISIS	0
PTE. MÁS DOC.	7
PTE. DECISIÓN	0
ARCHIVADA	14
EXPTE. POSIBLE INFRACCIÓN	0
CIERRE POR TRASLADO GIC	0
TOTAL	21