Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

INFORME BRECHAS SEGURIDAD DATOS PERSONALES

PRIMER SEMESTRE 2025

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

1. DESTACADO

La gestión adecuada de las brechas de seguridad de datos personales es esencial para proteger los derechos y libertades de las personas, en especial su derecho fundamental a la privacidad y a la protección de sus datos. Estas brechas constituyen incidentes que pueden derivar en la destrucción, pérdida o alteración —accidental o ilícita— de la información tratada por un responsable, así como en la comunicación o acceso no autorizados.

El RGPD[1] 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). Estas obligaciones tienen 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 la existencia de la brecha, permitirá también actuar a dichas personas en la defensa de sus intereses.

Las notificaciones de brechas de datos personales pueden dirigirse al Consejo a través de la Ventanilla Electrónica.

Del análisis de las brechas de seguridad de datos personales notificadas al Consejo durante el primer semestre año 2025, destacan las siguientes conclusiones:

- Mayor número de brechas: Ha habido un incremento notable, en línea con la tendencia general observada en otras autoridades de control.
- Las causas más notables de las brechas son:
    - Ciberataques: Este semestre se observa un significativo aumento de la relevancia de los ciberataques, especialmente aquellos relacionados con ransomware. Aunque su peso relativo en las estadísticas ha disminuido, los incidentes registrados han causado serias consecuencias en algunos municipios.

      Como actuación prioritaria las entidades públicas y sus proveedores deben cumplir con las medidas correspondientes del Esquema Nacional de Seguridad (ENS), acreditándolo mediante declaración o auditoría externa. Adicionalmente, deben adoptarse medidas específicas de protección de datos personales, como la privacidad desde el diseño y por defecto. Y en particular, para reducir estos

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).

incidentes, es clave mantener actualizados los sistemas operativos, aplicaciones y copias de seguridad, además de fortalecer las herramientas de detección y protección. Asimismo, la realización de análisis forenses tras un ataque facilita identificar las causas y aplicar mejoras oportunas. Cuando estos incidentes tengan un impacto significativo será obligatorio notificarlo al CCN-CERT (salvo que exista otro de referencia a nivel de administración autonómica o local), que puede prestar servicios de soporte remoto, coordinación operativa y asistencia técnica especializada (incluido el análisis forense).

- Errores en la publicación o notificación de información a los ciudadanos. Aunque no se ha registrado un aumento en el último semestre, continúan produciéndose numerosas brechas debido a errores en la difusión de información a la ciudadanía. Se recomienda implementar y reforzar procedimientos de revisión previos a la publicación o envío para prevenir estas situaciones.
- Es de destacar el aumento de las brechas que tienen origen en la pérdida y en el robo de dispositivos. Por ello, deben mantenerse y reforzarse las medidas de seguridad física y la concienciación sobre el uso de soportes portables o extraíbles.

- Se aprecia un disminución en las comunicaciones a los afectados de las brechas. Ello suele darse en las brechas que afectan a un número muy importantes de personas, evidenciando una cierta resistencia de los organismos a realizar este tipo de comunicaciones. Además, cuando estas comunicaciones tienen lugar suelen producirse con retrasos significativos, afectando negativamente a su eficacia. Por ello se realizan las siguientes recomendaciones:

  - Mejorar los procedimientos internos para agilizar la toma de decisiones y comunicar las brechas sin dilaciones indebidas.

  - En casos específicos como los ataques de ransomware, dada la potencial exfiltración de datos sensibles, es muy importante informar rápidamente a los afectados, ofreciendo recomendaciones preventivas concretas (por ejemplo, atención especial ante posibles fraudes o cambio de contraseñas).

  - La comunicación debe producirse incluso antes de finalizar el análisis completo del incidente, priorizando siempre la orientación preventiva sobre la mera información del evento.

  - Recordar que las incidencias que afectan únicamente a la disponibilidad de servicios

digitales (por ejemplo, sedes electrónicas o sitios web informativos) también pueden requerir comunicación pública, conforme a lo establecido en el artículo 33 del RGPD.

- 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.

- Número de ciudadanos afectados: En este semestre, han tenido lugar determinadas brechas que han afectado a un número muy importante de ciudadanos. A pesar de ello, en varias ocasiones, no se ha indicado el número de afectados por parte del Responsable del Tratamiento.
- Administraciones que notifican la brecha: Es particularmente relevante la disminución de notificaciones de brechas procedentes de la administración autonómica.
- Carencias en la gestión interna de brechas: En algunos casos se observa una gestión superficial de las brechas, sin profundizar adecuadamente en la investigación de sus causas ni en medidas preventivas efectivas. Es recomendable que las entidades revisen y mejoren sus procedimientos internos para asegurar una gestión más ágil, coordinada y con un claro enfoque preventivo. Especialmente en incidentes significativos, es necesario que los Responsables del Tratamiento desarrollen un análisis proactivo comprometiéndose a implementar mejoras concretas derivadas de dicho análisis.
- Resulta habitual 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 (al menos incluir si se trata de datos especialmente sensibles según el art 9 del RGPD)
  - su número (aunque sea aproximado). Este dato es particularmente importante para evaluar el impacto de las brechas de seguridad en la sociedad.
  - descripción de la brecha: tipo de brecha, posible vulnerabilidad del sistema aprovechada, efectos sobre los datos y sistemas, medidas de contención y recuperación.
  - descripción de las medidas correctivas adoptadas o propuestas

  Se recomienda, por ello, 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 seguri-

dad la obligación de notificar las brechas de seguridad de los datos personales (salvo las excepciones contempladas en el RGPD) 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 2025 en el Consejo de Transparencia y Protección de datos de Andalucía

PROVINCIA	
ALMERÍA	2
CÁDIZ	3
CÓRDOBA	2
GRANADA	1
HUELVA	1
JAÉN	2
MÁLAGA	11
SEVILLA	7
TOTAL	**29**

TIPO ENTIDAD	
ADMINISTRACIÓN AUTONÓMICA	4
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. AUTONÓMICA	3
ADMINISTRACIÓN LOCAL	19
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. LOCAL	2
SISTEMA UNIVERSITARIO ANDALUZ	1
TOTAL	**29**

CONTEXTO	
INTERNO (acción NO intencionada)	14
INTERNO (acción intencionada)	3
EXTERNO (acción NO intencionada)	2
EXTERNO (acción intencionada)	10
TOTAL	29

DIMENSIÓN AFECTADA *	
CONFIDENCIALIDAD	27
INTEGRIDAD	4
DISPONIBILIDAD	6

* una misma brecha puede afectar a varias dimensiones

MOTIVO PRINCIPAL	
ERROR	14
DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD	3
ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE	12
INCIDENCIA TÉCNICA	0
TOTAL	29

TIPO INCIDENTE	
INCIDENCIA TÉCNICA	1
DATOS PERSONALES MODIFICADOS/PERDIDOS/BORRADOS	0
ABUSO DE PRIVILEGIOS DE ACCESO	2
PUBLICACIÓN INDEBIDA	1
DATOS ENVIADOS /MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	3
REVELACIÓN INDEBIDA DE DATOS PERSONALES	11
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	4
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O UBICACIÓN INSEGURA O EXTRAVIADA EN ENTREGA POSTAL O ELIMINADA INDEBIDAMENTE	2
CIBERINCIDENTES: HACKING, MALWARE, RANSOMWARE, PHISHING	5
TOTAL	**29**

SEVERIDAD	
BAJA	19
MEDIA	8
ALTA	2
TOTAL	**29**

COMUNICACIÓN AFECTADOS POR RESP.TTO	
SÍ	11
NO SE VA A COMUNICAR	8
NO, PERO SE COMUNICARÁ	8
PDTE. DECISIÓN POR PARTE DE RESP. TRATAMIENTO	2
NO CONSTA	0
TOTAL	**29**

CATEGORÍAS DATOS ESPECIALES	
SÍ	6
NO	23
TOTAL	29

GÉNERO PERSONA QUE NOTIFICA	
HOMBRE	16
MUJER	13
ENTIDAD / NO CONSTA	0
TOTAL	29