Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

INFORME ANUAL BRECHAS SEGURIDAD DATOS PERSONALES 2025

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

1. Gestión de las brechas de seguridad de datos personales

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 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.

2. Análisis de las brechas notificadas durante el año 2025

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

2.1. Incremento del número de brechas notificadas

Ha habido un incremento relativo notable del número de brechas notificadas respecto al año 2024 (41% de incremento) aunque se sigue gestionando un número bajo de ellas (55 en el año 2025) en términos absolutos.

2.2. Causas más destacadas de las brechas

2.2.1. Ciberataques: en particular ransomware.

Si bien esta es la causa más destacada y de mayor repercusión, el número relativo de ciberataques notificados ha disminuido, a pesar de una tendencia general en sentido contrario.

En este sentido, debe advertirse del riesgo de infravalorar la importancia de los ciberataques en los que (aparentemente) no se ha producido exfiltración de datos. Aún en esos casos debe

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).

prestarse la debida atención a si la confidencialidad de los datos ha podido verse afectada, especialmente dado el elevado número de ciudadanos usualmente afectados.

Cabe destacar que en casi mitad de las brechas causadas por ciberataques no se indica el número de ciudadanos afectados. Debe tenerse en cuenta que este dato constituye uno de las principales indicadores de la gravedad de la brecha y es a la vez un elemento clave para el desarrollo de la responsabilidad proactiva.

Para prevenir este tipo de ataques, es esencial reforzar la seguridad de infraestructuras y servicios digitales, lo que incluye una vigilancia continua mediante registros (logs), auditorías y herramientas avanzadas de protección. Además, el Esquema Nacional de Seguridad debe aplicarse obligatoriamente en las entidades públicas y sus proveedores, junto con medidas de protección de datos por diseño y por defecto.

Si ocurre una brecha por ransomware, es recomendable acudir a especialistas para determinar las causas y las posibles consecuencias (en particular, exfiltraciones de datos). Por otra parte, dado que el ransomware suele dirigirse a la obtención de datos de la ciudadanía, conviene comunicar a los afectados con rapidez para que puedan adoptar medidas preventivas.

2.2.2. Errores en la publicación o notificación de información

Continúa la tendencia ascendente del número de brechas notificadas por este motivo, llegando a constituir el principal motivo de las brechas (un 40%) por lo que se recomienda establecer y reforzar los procedimientos de revisión antes de la salida de información, así como una mayor concienciación del personal que maneja datos personales.

2.2.3. Pérdida y robo de dispositivos

Es de destacar que se mantiene bajo el porcentaje de las brechas que tienen origen en la pérdida y en el robo de dispositivos. En todo caso, deben mantenerse las medidas de seguridad física y la concienciación sobre el uso de soportes portables o extraíbles.

2.3. Comunicación de brechas a los afectados

Se mantiene aproximadamente constante el porcentaje de brechas que se comunican a los afectados. No obstante, persiste una cierta resistencia en los organismos a comunicar a los afectados aquellas brechas que mayor riesgos pueden entrañar.

Igualmente, cuando se produce dicha comunicación a los ciudadanos, se observa un retraso en la misma, disminuyendo así su eficacia. Por ello, se recomienda a los organismos mejorar el procedimiento de toma de decisión de comunicación de brechas a los afectados para actuar sin

dilación indebida. Asimismo, se recuerda que se deben incluir recomendaciones específicas para que los ciudadanos puedan protegerse ante los efectos posibles de la brecha sobre ellos.

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.

2.4. Deficiencias en la gestión interna de las brechas

Es preciso indicar que en algunos casos, se gestionan las brechas solo de manera formal, pero sin investigar sus causas ni reseñar las medidas para evitar que vuelvan a producirse. En este sentido, 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.

2.5. Falta de detalle en la información notificada

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, así como su número;
- análisis de las posibles consecuencias de la brecha y como evitarlas en el futuro, en concreto para determinar si se produjeron exfiltraciones. En ocasiones el responsable se limita a reproducir el informe técnico del encargado del tratamiento, sin que se identifiquen acciones posteriores al respecto.

Por ello, 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.

3. Recomendación general sobre políticas de seguridad

Con carácter general, se recuerda que los organismos deben incluir en sus políticas de seguridad la obligación de notificar a la autoridad y comunicar a los afectados las brechas de seguridad de los datos personales (salvo las excepciones contempladas en el RGPD) y controlar su cumplimiento. Dichas políticas deben establecer asimismo procedimientos claros que definan las responsabilidades internas, los plazos de actuación y los canales de comunicación, de modo que cualquier incidente pueda ser detectado, evaluado y permita al organismo reaccionar con celeridad ante una brecha y adoptar las medidas necesarias para mitigar sus efectos.

4. Detalle de las Notificaciones de brechas

Seguidamente se muestran las principales estadísticas relativas a las notificaciones de brechas de datos personales notificadas al Consejo en virtud del artículo 33 del RGPD.

PROVINCIA	
ALMERÍA	2
CÁDIZ	6
CÓRDOBA	3
GRANADA	4
HUELVA	2
JAÉN	3
MÁLAGA	14
SEVILLA	21
TOTAL	55

TIPO ENTIDAD	
ADMINISTRACIÓN AUTONÓMICA	15
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. AUTONÓMICA	6
ADMINISTRACIÓN LOCAL	24
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. LOCAL	2
SISTEMA UNIVERSITARIO ANDALUZ	4
OTROS	4
TOTAL	55

CONTEXTO	
INTERNO (acción NO intencionada)	30
INTERNO (acción intencionada)	4
EXTERNO (acción NO intencionada)	2
EXTERNO (acción intencionada)	19
TOTAL	55

NÚMERO DE CIUDADANOS AFECTADOS	Brechas	Afectados
1	10	10
2-10	9	39
11-100	10	582
101-1000	11	4297
1001-10000	1	6000
MÁS DE 10000	2	64055
NÚMERO NO INDICADO (CIBERINCIDENTES)	6	
NÚMERO NO INDICADO (NO CIBERINCIDENTES)	6	
TOTAL …..	55	74983
	Mediana	31

DIMENSIÓN AFECTADA *	
CONFIDENCIALIDAD	53
INTEGRIDAD	5
DISPONIBILIDAD	8

* una misma brecha puede afectar a varias dimensiones

SEVERIDAD	
BAJA	38
MEDIA	14
ALTA	3
TOTAL …..	55

CATEGORÍAS DATOS ESPECIALES	
SÍ	12
NO	43
TOTAL …..	55

TIPO INCIDENTE	
INCIDENCIA TÉCNICA	6
DATOS PERSONALES MODIFICADOS/PERDIDOS/BORRADOS	0
ABUSO DE PRIVILEGIOS DE ACCESO	3
ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO	5
PUBLICACIÓN INDEBIDA	7
DATOS ENVIADOS /MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	13
REVELACIÓN INDEBIDA DE DATOS PERSONALES	1
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	4
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O UBICACIÓN INSEGURA O EXTRAVIADA EN ENTREGA POSTAL O ELIMINADA INDEBIDAMENTE	3
CIBERINCIDENTES: HACKING, MALWARE, RANSOMWARE, PHISHING	13
TOTAL	**55**

COMUNICACIÓN AFECTADOS POR RESP.TTO	
SÍ	24
NO SE VA A COMUNICAR	12
NO, PERO SE COMUNICARÁ	13
PDTE. DECISIÓN POR PARTE DE RESP. TRATAMIENTO	6
NO CONSTA	0
TOTAL	**55**

GÉNERO PERSONA QUE NOTIFICA	
HOMBRE	38
MUJER	17
ENTIDAD / NO CONSTA	0
TOTAL	**55**

HISTÓRICO DE BRECHAS	AÑO							TOTAL
SITUACIÓN	2019	2020	2021	2022	2023	2024	2025	
PTE. ACUSE	0	0	0	0	0	0	0	0
PTE. ANÁLISIS	0	0	0	0	0	0	0	0
PTE. MÁS DOC POR RESP.TTO	0	0	0	0	0	7	2	9
PTE. DECISIÓN	0	0	0	0	0	0	0	0
ARCHIVADA	5	22	36	34	43	30	49	219
EXPTE. POSIBLE INFRACCIÓN	0	0	0	0	0	0	0	0
CIERRE POR TRASLADO GIC	0	0	0	4	5	2	4	15
TOTAL	5	22	36	38	48	39	55	243
No es competencia del CTPDA	0	0	2	0	3	2	2	9