Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

# INFORME ANUAL BRECHAS SEGURIDAD DATOS PERSONALES 2024

## 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 año 2024, destacan las **siguientes conclusiones:**

- **Mayor número de personas afectadas:** A pesar de la disminución en el número de brechas respecto al año anterior, algunas de las notificadas en el año 2024 han afectado a un número muy elevado de ciudadanos.
- Las **causas más notables** de las brechas son:
    - Ciberataques: en particular **ransomware.** 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 privacidad por diseño y por defecto.

      Si ocurre una brecha por ransomware, es clave acudir a especialistas en análisis forense para determinar posibles exfiltraciones de datos. Asimismo, se debe informar al CERT competente. Dado que el ransomware suele dirigirse a la

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).

obtención de datos de la ciudadanía, conviene comunicar a los afectados con rapidez para que puedan adoptar medidas preventivas.

- **Errores en la publicación o notificación** de información a los ciudadanos. Se evidencia el aumento de brechas por este motivo, por lo que se recomienda establecer y reforzar procedimientos de revisión antes de la salida de información.
- **Pérdida de documentación en la entrega postal.** Se ha advertido también un incremento en esta tipología de brechas, por lo que debería reforzarse el seguimiento de los envíos.
- Es de destacar una **reducción** 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.

- Se aprecia un **aumento en las comunicaciones a los afectados** de las brechas. 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 **cierto 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 les advierte que deben incluirse 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.
- Respecto a años anteriores, se ha producido un **notable incremento de la participación de las mujeres** en las notificaciones al Consejo en 2024.
- Es preciso indicar que en algunos casos, se **gestionan las brechas solo de manera formal**, sin investigar sus causas ni como 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.

- 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**, 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**.

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 (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 año 2024 en el Consejo de Transparencia y Protección de datos de Andalucía

| PROVINCIA | |
|---|---|
| ALMERÍA | 1 |
| CÁDIZ | 1 |
| CÓRDOBA | 5 |
| GRANADA | 1 |
| HUELVA | 4 |
| JAÉN | 0 |
| MÁLAGA | 9 |
| SEVILLA | 18 |
| **TOTAL .....** | **39** |

| TIPO ENTIDAD | |
|---|---|
| ADMINISTRACIÓN AUTONÓMICA | 14 |
| ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. AUTONÓMICA | 5 |
| ADMINISTRACIÓN LOCAL | 10 |
| ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE ADMON. LOCAL | 7 |
| SISTEMA UNIVERSITARIO ANDALUZ | 3 |
| **TOTAL .....** | **39** |

| CONTEXTO | |
|---|---|
| INTERNO (acción NO intencionada) | 20 |
| INTERNO (acción intencionada) | 3 |
| EXTERNO (acción NO intencionada) | 5 |
| EXTERNO (acción intencionada) | 11 |
| TOTAL ..... | 39 |

| Número de ciudadanos afectados | Brechas | Afectados |
|---|---|---|
| 1 | 8 | 8 |
| 2-100 | 7 | 309 |
| 100-1.000 | 9 | 2.122 |
| 1.000-10.000 | 2 | 2.432 |
| Más de 10.000 | 2 | 161.450 |
| Número indeterminado | 11 | - |
| TOTAL ..... | 39 | 166.321 |

| DIMENSIÓN AFECTADA * | |
|---|---|
| CONFIDENCIALIDAD | 33 |
| INTEGRIDAD | 1 |
| DISPONIBILIDAD | 10 |

* una misma brecha puede afectar a varias dimensiones

| MOTIVO PRINCIPAL | |
|---|---|
| ERROR | 11 |
| DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD | 8 |
| ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE | 15 |
| INCIDENCIA TÉCNICA | 5 |
| TOTAL ..... | 39 |

| TIPO INCIDENTE | |
|---|---|
| INCIDENCIA TÉCNICA | 5 |
| DATOS PERSONALES MODIFICADOS/PERDIDOS/BORRADOS | 0 |
| ABUSO DE PRIVILEGIOS DE ACCESO | 0 |
| PUBLICACIÓN INDEBIDA | 7 |
| DATOS ENVIADOS /MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE) | 7 |
| REVELACIÓN INDEBIDA DE DATOS PERSONALES | 2 |
| DISPOSITIVO PERDIDO, ROBADO O DESECHADO | 2 |
| DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O UBICACIÓN INSEGURA O EXTRAVIADA EN ENTREGA POSTAL O ELIMINADA INDEBIDAMENTE | 5 |
| CIBERINCIDENTES: HACKING, MALWARE, RANSOMWARE, PHISHING | 11 |
| **TOTAL .....** | **39** |

| SEVERIDAD | |
|---|---|
| BAJA | 23 |
| MEDIA | 12 |
| ALTA | 4 |
| **TOTAL .....** | **39** |

| COMUNICACIÓN AFECTADOS POR RESP.TTO | |
|---|---|
| SÍ | 20 |
| NO SE VA A COMUNICAR | 5 |
| NO, PERO SE COMUNICARÁ | 5 |
| PDTE. DECISIÓN POR PARTE DE RESP. TRATAMIENTO | 8 |
| NO CONSTA | 1 |
| **TOTAL .....** | **39** |

| CATEGORÍAS DATOS ESPECIALES | |
|---|---|
| SÍ | **12** |
| NO | **27** |
| **TOTAL .....** | **39** |

| GÉNERO PERSONA QUE NOTIFICA | |
|---|---|
| HOMBRE | **18** |
| MUJER | **21** |
| ENTIDAD / NO CONSTA | **0** |
| **TOTAL .....** | **39** |

| HISTÓRICO DE BRECHAS | AÑO | | | | | | TOTAL |
|---|---|---|---|---|---|---|---|
| **SITUACIÓN** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | |
| PTE. ACUSE | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| PTE. ANÁLISIS | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| PTE. MÁS DOC POR RESP.TTO | 0 | 0 | 0 | 0 | 0 | 7 | **7** |
| PTE. DECISIÓN | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| ARCHIVADA | 5 | 22 | 34 | 34 | 40 | 30 | **165** |
| EXPTE. POSIBLE INFRACCIÓN | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| CIERRE POR TRASLADO GIC | 0 | 0 | 0 | 4 | 5 | 2 | **11** |
| **TOTAL .....** | **5** | **22** | **34** | **38** | **45** | **39** | **183** |
| No es competencia del CTPDA | 0 | 0 | 2 | 0 | 3 | 2 | **7** |