Abril 2025
Notificaciones de Brechas de Datos Personales

Agencia Española de Protección de Datos
División de Innovación Tecnológica
Mayo 2025

1. DESTACADO

Una causa frecuente de brechas de confidencialidad es el uso de credenciales comprometidas en brechas de datos personales que permiten el acceso a otros sistemas de información y exfiltrar datos personales. La reutilización de credenciales en varios sistemas facilita la labor de los atacantes. Es frecuente la utilización de credenciales comprometidas de algún empleado para vulnerar aplicaciones o servicios web expuestos en internet o la VPN corporativa.

Los responsables del tratamiento deben adoptar medidas técnicas y organizativas adecuadas al nivel de riesgo de sus tratamientos y exigir a sus encargados de tratamiento la adopción de tales medidas. Sin ánimo de exhaustividad, algunas de las medidas recomendadas son:

- Implantar autenticación de factor múltiple en aplicaciones/servicios expuestos en internet (como mínimo en para las cuentas privilegiadas o de administración) y en VPN corporativas. Preferiblemente basada en certificados.

- Exponer en Internet únicamente aquellas aplicaciones/servicios a los que sea imprescindible acceder desde el exterior, siendo preferible el acceso desde VPN corporativa.

- Deshabilitar permisos de administración o roles mas altos si el acceso se realiza desde Internet, cuando sea posible.

- Restringir el acceso a aplicaciones/servicios web y a la VPN corporativa por geobloqueo de IPs (por ejemplo, restringir el acceso desde IPs fuera de España o de la UE y habilitar el acceso de forma excepcional a países concretos para casos de viajes de trabajo concretos), IPs de redes de anonimización (p.ej. TOR) e IPs de proveedores de acceso por VPN.

- Establecer una política estricta de contraseñas que obligue a establecer contraseñas robustas, prohíba la reutilización de contraseñas y obligue a la utilización de gestores de contraseñas.

- Contar con un servicio de vigilancia activa de credenciales comprometidas vinculadas al dominio de la organización.

- Establecer cuotas de acceso a datos que impidan descargas masivas y generen alertas.

- Permitir el acceso a aplicaciones/servicios web y a la VPN corporativa únicamente desde dispositivos corporativos o autorizados. Impedir el acceso desde dispositivos personales.

- Segmentar la redes internas así como los almacenes de datos.

- Adecuar las medidas adoptadas al riesgo que para los derechos fundamentales implica una brecha en cada uno de los tratamientos de la organización.

- 217 notificaciones recibidas, 210 de ellas a través del formulario en Sede Electrónica[1].
- 64 son notificaciones con información adicional.

[1] Las siguientes cifras se refieren exclusivamente a las notificaciones recibidas mediante el formulario de notificación de brechas de datos personales en Sede Electrónica.

- 179 notificaciones por parte de organizaciones del ámbito privado.
- 192 notificaciones indican brecha de confidencialidad, 13 de integridad y 58 de disponibilidad (algunas brechas presentan más de una tipología).
- 142 notificaciones indican origen externo.
- 131 notificaciones indican carácter malintencionado.
- 40 notificaciones de brechas implican categorías especiales de datos, de las cuales 39 se refieren a datos de salud.
- 139 notificaciones indican severidad de las consecuencias para los afectados baja.
- 1 notificaciones indican severidad muy alta.
- 22 notificaciones de brechas con implicaciones de carácter transfronterizo.
- La notificación de brecha con mayor número de afectados indica aproximadamente 17750000 personas afectadas.
- 75 notificaciones indican haber comunicado la brecha en total a aproximadamente 17251153 personas.
- 51 notificaciones indican que comunicarán la brecha en total a aproximadamente 618972 afectados.
- 52 notificaciones indican que no informarán a los afectados.

2. DETALLE DE NOTIFICACIONES

En este informe se resumen las características principales de las notificaciones de brechas de datos personales recibidas en la Agencia Española de Protección de Datos (AEPD) en virtud del artículo 33 del Reglamento (UE) 2016/679, General de Protección de Datos.

El informe recoge las notificaciones de brechas de datos personales recibidas durante abril de 2025, siendo un total de 217 notificaciones, de las cuales 210 han utilizado como canal de comunicación el formulario de "notificación de brechas de datos personales" publicado en la sede electrónica.

Los datos indicados en este apartado corresponden al contenido de las notificaciones de datos personales recibidas exclusivamente a través del formulario en Sede Electrónica.

Entrada de notificaciones:

Descripción	Total
Notificaciones recibidas	217
Formulario sede electrónica	210
Otros medios	7

Evolución notificaciones[2]:

	Total
Total 2023	**2005**
Total 2024	**2933**
Acumulado últimos 12 meses	**2758**
abr-24	228
may-24	462
jun-24	347
jul-24	227
ago-24	155
sep-24	160
oct-24	213
nov-24	196
dic-24	162
ene-25	165
feb-25	193
mar-25	261
abr-25	**217**

[2] Estas cifras se refieren al total de notificaciones recibidas por cualquier canal de comunicación.

Tipo de notificación:

Tipo	Total
Nueva	146
Inicial	80
Completa	66
Modificación	64

Tipo de organización:

Descripción	Total
Organizaciones privadas	179
Organizaciones públicas	31

Tipología de la brecha de datos personales:

Tipo	Total
Confidencialidad	192
Integridad	13
Disponibilidad	58

Tratamiento de las brechas de datos personales:

Descripción	Total
Resueltas	132
No resueltas o no indicado	78

Medios de materialización de las brechas de datos personales:

Medios	Total
Revelación verbal no autorizada	1
Documentación perdida, robada	21
Correo postal perdido, abierto	7
Eliminación incorrecta de datos en formato papel	0
Datos enviados por error (postal o electrónicamente)	30
Datos personales eliminados / destruidos	2
Abuso de privilegios de acceso	3
Datos residuales en dispositivos obsoletos	0
Publicación no intencionada / autorizada	10
Envío de correo electrónico a múltiples destinatarios sin cco	5
Dispositivo perdido o robado	8
Ciberincidente: Dispositivo cifrado / secuestro de información	64
Ciberincidente: Suplantación de identidad (phishing)	31
Ciberincidente: Acceso no autorizado a datos en sistema de información	79
Incidencia técnica	13
Modificación no autorizada de datos	3
Datos personales mostrados al individuo incorrecto	18

Contexto de la brecha de datos personales:

Origen / Intencionalidad	Total
Interno Responsable	48
Interno Encargado	20
Externo	142
Accidental	70
Malintencionado	131
Intencionalidad desconocida	9

Categorías de datos:

Categorías	Total
Categorías Especiales	40
Condenas e inf. penales	4

Detalle categorías especiales:

Medios	Total
Sobre la religión o creencia	3
Sobre el origen racial	4
Sobre la opinión política	0
De salud	39
Sobre la afiliación sindical	2
Sobre la vida sexual	2
Genéticos	1
Biométricos	2

Perfiles de los afectados:

Afectados	Total
Clientes / Ciudadanos	134
Estudiantes / Alumnos	8
Usuarios	30
Pacientes	8
Suscriptores / Clientes potenciales	13
Afiliados / Asociados	6
Militares / Policía	0
Empleados	93
Otros	30

Severidad de las consecuencias para los interesados:

Severidad	Total
Baja	139
Media	33
Alta	11
Muy alta	1
Desconocida	26

Número de afectados:

Afectados	Total
[0-99]	93
[100-999]	61
[1000-9999]	34
[10000-99999]	10
[100000-999999]	9
[1000000-99999999]	3

Evolución comunicaciones a los interesados:

	Han sido informados[3] o Serán informados[4] (cifra aproximada)
Total 2023	**36.572.000**
Total 2024	**100.103.000**
Acumulado últimos 12 meses	**130.719.000**
abr-24	5.110.000
may-24	30.508.000
jun-24	10.400.000
jul-24	11.034.000
ago-24	1.303.000
sep-24	7.755.000
oct-24	20.661.000
nov-24	1.257.000
dic-24	1.019.000
ene-25	551.000
feb-25	3.798.000
mar-25	24.563.000
abr-25	**17.870.000**

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	Total
Andalucía	17
Aragón	5
Principado de Asturias	0
Baleares	5
Cantabria	1
Castilla y León	6
Castilla-La Mancha	4
Cataluña	40
Comunidad Valenciana	19
Extremadura	1
Galicia	8
Comunidad de Madrid	76
Región de Murcia	3
Comunidad Foral de Navarra	7
País Vasco	13
La Rioja	0
Canarias	3
Ceuta	0
Melilla	0

[3] En la notificación de brecha de datos personales se indica que los interesados han sido informados.
[4] En la notificación de brecha de datos personales se indica que los interesados serán informados.

Implicaciones transfronterizas:

Notificaciones con afectados en otros Estados Miembro: 22

Estado	Total
ALEMANIA	15
AUSTRIA	7
BELGICA	10
BULGARIA	8
REPÚBLICA CHECA	6
CHIPRE	3
CROACIA	4
DINAMARCA	5
FRANCIA	13
ESLOVAQUIA	4
ESLOVENIA	4
ESTONIA	4
FINLANDIA	4

Estado	Total
GRECIA	4
HUNGRIA	5
IRLANDA	6
ITALIA	12
LETONIA	6
LITUANIA	4
LUXEMBURGO	6
MALTA	3
PAISES BAJOS	9
PORTUGAL	14
RUMANIA	6
SUECIA	5
POLONIA	8