Septiembre 2023
Notificaciones de Brechas de Datos Personales

Agencia Española de Protección de Datos
División de Innovación Tecnológica
Octubre 2023

1. DESTACADO

Una causa frecuente de brechas de confidencialidad es el uso de credenciales comprometidos en otras brechas de datos personales para comprometer 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 exahaustividad, 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 aquellos 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.

- 148 notificaciones recibidas, 145 de ellas a través del formulario en Sede Electrónica[1].
- 36 son notificaciones con información adicional.
- 113 notificaciones por parte de organizaciones del ámbito privado.
- 135 notificaciones indican brecha de confidencialidad, 4 de integridad y 24 de disponibilidad (algunas brechas presentan más de una tipología).
- 83 notificaciones indican origen externo.
- 84 notificaciones indican carácter malintencionado.

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

- 30 notificaciones de brechas implican categorías especiales de datos, de las cuales 27 se refieren a datos de salud.
- 114 notificaciones indican severidad de las consecuencias para los afectados baja.
- 1 notificaciones indican severidad muy alta.
- 7 notificaciones de brechas con implicaciones de carácter transfronterizo.
- La notificación de brecha con mayor número de afectados indica aproximadamente 1600000 personas afectadas.
- 55 notificaciones indican haber comunicado la brecha en total a aproximadamente 1631730 personas.
- 32 notificaciones indican que comunicarán la brecha en total a aproximadamente 258710 afectados.
- 47 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 septiembre de 2023, siendo un total de 148 notificaciones, de las cuales 145 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	148
Formulario sede electrónica	145
Otros medios	3

Evolución notificaciones[2]:

	Total
Total 2021	**1647**
Total 2022	**1751**
Acumulado últimos 12 meses	**1994**
sep-22	189
oct-22	166
nov-22	209
dic-22	170
ene-23	142
feb-23	149
mar-23	208
abr-23	214
may-23	158
jun-23	184
jul-23	135
ago-23	111
sep-23	**148**

Tipo de notificación:

Tipo	Total
Nueva	109
Inicial	42
Completa	67
Modificación	36

Tipo de organización:

Descripción	Total
Organizaciones privadas	113
Organizaciones públicas	32

Tipología de la brecha de datos personales:

Tipo	Total
Confidencialidad	135
Integridad	4
Disponibilidad	24

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

Tratamiento de las brechas de datos personales:

Descripción	Total
Resueltas	101
No resueltas o no indicado	44

Medios de materialización de las brechas de datos personales:

Medios	Total
Revelación verbal no autorizada	4
Documentación perdida, robada	13
Correo postal perdido, abierto	7
Eliminación incorrecta de datos en formato papel	0
Datos enviados por error (postal o electrónicamente)	16
Datos personales eliminados / destruidos	0
Abuso de privilegios de acceso	6
Datos residuales en dispositivos obsoletos	1
Publicación no intencionada / autorizada	16
Envío de correo electrónico a múltiples destinatarios sin cco	6
Dispositivo perdido o robado	9
Ciberincidente: Dispositivo cifrado / secuestro de información	25
Ciberincidente: Suplantación de identidad (phishing)	22
Ciberincidente: Acceso no autorizado a datos en SI	43
Incidencia técnica	3
Modificación no autorizada de datos	1
Datos personales mostrados al individuo incorrecto	7

Contexto de la brecha de datos personales:

Origen / Intencionalidad	Total
Interno Responsable	46
Interno Encargado	16
Externo	83
Accidental	57
Malintencionado	84
Intencionalidad desconocida	4

Categorías de datos:

Categorías	Total
Categorías Especiales	30
Condenas e inf. penales	1

Detalle categorías especiales:

Medios	Total
Sobre la religión o creencia	1
Sobre el origen racial	2
Sobre la opinión política	0
De salud	27
Sobre la afiliación sindical	6
Sobre la vida sexual	1
Genéticos	0
Biométricos	1

Perfiles de los afectados:

Afectados	Total
Clientes / Ciudadanos	95
Estudiantes / Alumnos	7
Usuarios	25
Pacientes	11
Suscriptores / Clientes potenciales	8
Afiliados / Asociados	4
Militares / Policía	1
Empleados	56
Otros	17

Severidad de las consecuencias para los interesados:

Severidad	Total
Baja	114
Media	19
Alta	7
Muy alta	1
Desconocida	4

Número de afectados:

Afectados	Total
[0-99]	71
[100-999]	32
[1000-9999]	31
[10000-99999]	7
[100000-999999]	3
[1000000-99999999]	1

Evolución comunicaciones a los interesados:

	Han sido informados[3] o Serán informados[4] (cifra aproximada)
Total 2021	**12.996.000**
Total 2022	**30.828.000**
Acumulado últimos 12 meses	**19.032.000**
sep-22	375.000
oct-22	4.466.000
nov-22	2.668.000
dic-22	2.371.000
ene-23	141.000
feb-23	256.000
mar-23	1.390.000
abr-23	3.029.000
may-23	312.000
jun-23	181.000
jul-23	656.000
ago-23	1.671.000
sep-23	**1.891.000**

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	Total
Andalucía	14
Aragón	3
Principado de Asturias	0
Baleares	0
Cantabria	3
Castilla y León	2
Castilla-La Mancha	5
Cataluña	28
Comunidad Valenciana	10
Extremadura	0
Galicia	10
Comunidad de Madrid	54
Región de Murcia	1
Comunidad Foral de Navarra	1
País Vasco	9
La Rioja	1
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: 7

Estado	Total
ALEMANIA	4
AUSTRIA	2
BELGICA	4
BULGARIA	2
REPÚBLICA CHECA	2
CHIPRE	1
CROACIA	1
DINAMARCA	1
FRANCIA	6
ESLOVAQUIA	1
ESLOVENIA	1
ESTONIA	1
FINLANDIA	1

Estado	Total
GRECIA	1
HUNGRIA	1
IRLANDA	2
ITALIA	4
LETONIA	0
LITUANIA	1
LUXEMBURGO	2
MALTA	1
PAISES BAJOS	4
PORTUGAL	5
RUMANIA	2
SUECIA	2
POLONIA	2