

Enero 2023

Notificaciones de Brechas de Datos Personales

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

1. DESTACADO

En los últimos meses se suceden notificaciones de brechas relativas al compromiso de credenciales de acceso de establecimientos hoteleros (responsables del tratamiento) en portales de gestión de reservas en Internet (que actúan como encargados de tratamiento), resultando en el acceso de terceros a datos personales de los clientes que han realizado reservas en el hotel a través de esos portales de reservas.

Esos datos personales, incluyendo la información de la reserva, son utilizados por los cibercriminales para contactar con los clientes a través de los portales de reserva, correo electrónico y otros servicios de mensajería instantánea, alegando problemas en el pago y reclamando el pago de la reserva. Es decir, los datos se utilizan para ejecutar intentos de fraude que en muchas ocasiones tienen éxito, con el consiguiente perjuicio para las personas afectadas.

Además de los posibles delitos en los que los cibercriminales incurren (suplantación de identidad y fraude, entre otros) y que el responsable debe denunciar siempre ante las autoridades policiales y/o judiciales, esto supone una brecha de datos personales que también deben gestionar de acuerdo al RGPD.

Esto incluye documentar la brecha y la respuesta dada para resolverla, notificarla a la Autoridad de Control conforme al art. 33 del RGPD y comunicar la brecha a los interesados afectados conforme al art. 34 del RGPD al suponer un alto riesgo para los derechos y libertades de las personas.

Además, conforme al art. 32 del RGPD responsables y encargados deben implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo. Por ejemplo la implementación de sistemas de autenticación de doble factor efectivos en los servicios de reserva implementados por los encargados y la obligación de los responsables de utilizar estos sistemas de autenticación reforzada adecuadamente.

Así mismo, corresponde al responsable del tratamiento la obligación de únicamente seleccionar aquellos encargados del tratamiento que puedan garantizar un nivel adecuado de seguridad y el cumplimiento de la normativa de protección de datos. Esto es, los establecimientos hoteleros únicamente deben utilizar aquellos servicios de gestión de reservas que puedan garantizar un nivel de seguridad adecuado para los datos personales de sus clientes.

- 142 notificaciones recibidas, 130 de ellas a través del formulario en Sede Electrónica¹.
- 37 son notificaciones con información adicional.
- 111 notificaciones por parte de organizaciones del ámbito privado.
- 115 notificaciones indican brecha de confidencialidad, 6 de integridad y 31 de disponibilidad (algunas brechas presentan más de una tipología).
- 84 notificaciones indican origen externo.
- 74 notificaciones indican carácter malintencionado.
- 29 notificaciones de brechas implican categorías especiales de datos, de las cuales 25 se refieren a datos de salud.
- 97 notificaciones indican severidad de las consecuencias para los afectados baja.
- 1 notificaciones indican severidad muy alta.
- 14 notificaciones de brechas con implicaciones de carácter transfronterizo.
- La notificación de brecha con mayor número de afectados indica aproximadamente 12000000 personas afectadas.
- 38 notificaciones indican haber comunicado la brecha en total a aproximadamente 96035 personas.
- 32 notificaciones indican que comunicarán la brecha en total a aproximadamente 44712 afectados.
- 45 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 enero de 2023, siendo un total de 142 notificaciones, de las cuales 130 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	142
Formulario sede electrónica	130
Otros medios	12

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

Evolución notificaciones²:

	Total
Total 2021	1647
Total 2022	1751
Acumulado últimos 12 meses	1777
ene-22	116
feb-22	143
mar-22	140
abr-22	114
may-22	127
jun-22	102
jul-22	94
ago-22	181
sep-22	189
oct-22	166
nov-22	209
dic-22	170
ene-23	142

Tipo de notificación:

Tipo	Total
Nueva	93
Inicial	38
Completa	55
Modificación	37

Tipo de organización:

Descripción	Total
Organizaciones privadas	111
Organizaciones públicas	19

Tipología de la brecha de datos personales:

Tipo	Total
Confidencialidad	115
Integridad	6
Disponibilidad	31

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	89
No resueltas o no indicado	41

Medios de materialización de las brechas de datos personales:

Medios	Total
Revelación verbal no autorizada	0
Documentación perdida, robada	16
Correo postal perdido, abierto	0
Eliminación incorrecta de datos en formato papel	0
Datos enviados por error (postal o electrónicamente)	18
Datos personales eliminados / destruidos	0
Abuso de privilegios de acceso	3
Datos residuales en dispositivos obsoletos	0
Publicación no intencionada / autorizada	7
Envío de correo electrónico a múltiples destinatarios sin cco	4
Dispositivo perdido o robado	14
Ciberincidente: Dispositivo cifrado / secuestro de información	24
Ciberincidente: Suplantación de identidad (phishing)	23
Ciberincidente: Acceso no autorizado a datos en SI	44
Incidencia técnica	7
Modificación no autorizada de datos	2
Datos personales mostrados al individuo incorrecto	11

Contexto de la brecha de datos personales:

Origen / Intencionalidad	Total
Interno Responsable	38
Interno Encargado	8
Externo	84
Accidental	50
Malintencionado	74
Intencionalidad desconocida	6

Categorías de datos:

Categorías	Total
Categorías Especiales	29
Condenas e inf. penales	2

Detalle categorías especiales:

Medios	Total
Sobre la religión o creencia	0
Sobre el origen racial	1
Sobre la opinión política	2
De salud	25
Sobre la afiliación sindical	3
Sobre la vida sexual	1
Genéticos	0
Biométricos	1

Perfiles de los afectados:

Afectados	Total
Clientes / Ciudadanos	87
Estudiantes / Alumnos	10
Usuarios	30
Pacientes	12
Suscriptores / Clientes potenciales	3
Afiliados / Asociados	4
Militares / Policía	0
Empleados	42
Otros	16

Severidad de las consecuencias para los interesados:

Severidad	Total
Baja	97
Media	11
Alta	12
Muy alta	1
Desconocida	9

Número de afectados:

Afectados	Total
[0-99]	51
[100-999]	42
[1000-9999]	20
[10000-99999]	12
[100000-999999]	3
[1000000-99999999]	2

Evolución comunicaciones a los interesados (en miles):

	Han sido informados ³	Serán informados ⁴
Total 2021	11067	1929
Total 2022	19774	11054
Acumulado últimos 12 meses	19835	10787
ene-22	35	312
feb-22	15	182
mar-22	132	3017
abr-22	1614	18
may-22	6087	619
jun-22	6356	58
jul-22	29	40
ago-22	1214	1220
sep-22	324	51
oct-22	747	3719
nov-22	970	1698
dic-22	2251	120
ene-23	96	45

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.

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	Total
Andalucía	10
Aragón	1
Principado de Asturias	4
Baleares	2
Cantabria	2
Castilla y León	6
Castilla-La Mancha	1
Cataluña	21
Comunidad Valenciana	11
Extremadura	3
Galicia	7
Comunidad de Madrid	52
Región de Murcia	2
Comunidad Foral de Navarra	0
País Vasco	6
La Rioja	0
Canarias	2
Ceuta	0
Melilla	0

Implicaciones transfronterizas:

Notificaciones con afectados en otros Estados Miembro: 14

Estado	Total	Estado	Total
ALEMANIA	9	GRECIA	3
AUSTRIA	3	HUNGRÍA	4
BELGICA	5	IRLANDA	4
BULGARIA	2	ITALIA	9
REPÚBLICA CHECA	3	LETONIA	0
CHIPRE	0	LITUANIA	1
CROACIA	0	LUXEMBURGO	3
DINAMARCA	3	MALTA	0
FRANCIA	7	PAISES BAJOS	7
ESLOVAQUIA	2	PORTUGAL	6
ESLOVENIA	0	RUMANIA	1
ESTONIA	2	SUECIA	4
FINLANDIA	5	POLONIA	5