Consejo de Transparencia
y Protección de Datos
de Andalucía

INFORME SOBRE BRECHAS SEGURIDAD DE LOS DATOS PERSONALES

PRIMER SEMESTRE 2023

CONTENIDO

1 DESTACADO

La **gestión adecuada de las brechas de datos personales** como incidentes de seguridad que pueden ocasionar la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos, es esencial para salvaguardar los derechos y libertades de las personas físicas, concretamente el derecho fundamental a la privacidad y a la protección de los datos personales.

El RGPD impone a los responsables del tratamiento la **obligación de notificar las brechas** a las autoridades de control competentes y en situaciones que puedan suponer alto riesgo, **comunicarlas a los interesados** afectados. Esta obligación tiene 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 las existencia de la brecha, permitirá también actuar a dichas personas en la defensa de sus intereses.

Del **análisis de las brechas** de seguridad de datos personales notificadas al Consejo durante el primer semestre de 2023, los datos más relevantes a **destacar son los siguientes:**

- Se han observado casos en los que las brechas se gestionan con una visión eminentemente formal, sin abordar los motivos que la causaron y sin una plena involucración del responsable del tratamiento. En consecuencia, se recomienda a los organismos la **revisión del procedimiento** de gestión de brechas de seguridad, a fin de dotarlo de **mayor agilidad**, **mayor seguimiento y coordinación** de las acciones realizadas.
- Se detecta **cierta resistencia de los organismos** afectados a comunicar a los interesados las brechas que pueden suponer un alto riesgo para los mismos. Se recomienda a los organismos **mejorar el procedimiento de toma de decisión de comunicación** de brechas de seguridad a los interesados, **particularmente el análisis de riesgos derivados de la misma**, para **actuar sin dilación indebida.**
- Es frecuente 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**.

- Una de las causas más frecuentes de brecha es la pérdida o robo de dispositivos. Es necesario **reforzar la seguridad de los dispositivos físicos que contienen datos personales.**

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 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 y recibidas en el Consejo en virtud del artículo 33 del RGPD.

SITUACIÓN	
RESUELTAS O ARCHIVADAS	14
PENDIENTES DE RESOLVER	6
TOTAL	20

CONTEXTO	
INTERNO (ACCIÓN NO INTENCIONADA)	6
INTERNO (ACCIÓN INTENCIONADA)	0
EXTERNO (ACCIÓN NO INTENCIONADA)	1
EXTERNO (ACCIÓN INTENCIONADA)	13
TOTAL	20

PROVINCIA	
ALMERÍA	3
CÁDIZ	2
CÓRDOBA	1
GRANADA	3
HUELVA	1
MÁLAGA	1
SEVILLA	9
TOTAL	20

DIMENSIÓN AFECTADA	
CONFIDENCIALIDAD	17
INTEGRIDAD	2
DISPONIBILIDAD	5

PERSONA QUE NOTIFICA	
HOMBRE	16
MUJER	4
TOTAL	20

TIPO ENTIDAD	
ADMINISTRACIÓN AUTONÓMICA	9
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. AUTONÓMICA	2
ADMINISTRACIÓN LOCAL	5
ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMON. LOCAL	2
SISTEMA UNIVERSITARIO ANDALUZ	2
TOTAL	20

MOTIVO PRINCIPAL	
ERROR	2
DESCONOCIMIENTO / OMISIÓN / INCUMPLIMIENTO NORMATIVA O MEDIDAS DE SEGURIDAD	5
ATAQUE / PERDIDA / ROBO / CIBERINCIDENTE	13
TOTAL	20

TIPO DE INCIDENTE	
ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO	1
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	2
REVELACIÓN INDEBIDA DE DATOS PERSONALES	2
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	7
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O EN LOCALIZACIÓN INSEGURA O ELIMINADA INCORRECTAMENTE	1
CIBERINCIDENTE: HACKING, MALWARE O PHISHING	7
TOTAL	**20**

TIPOLOGÍA DATOS AFECTADOS	
CATEGORÍAS ESPECIALES DE DATOS PERSONALES	7
RESTO DE CATEGORÍAS DE DATOS PERSONALES	13
TOTAL	**20**

SEVERIDAD	
BAJA	11
MEDIA	2
ALTA	5
MUY ALTA	0
DESCONOCIDA	2
TOTAL	**20**

COMUNICACIÓN AFECTADOS	
DECISIÓN COMUNICAR	2
DECISIÓN NO COMUNICAR	13
SIN CONFIRMAR	5
TOTAL	**20**

3 BRECHA DESTACADA DEL SEMESTRE

En el siguiente apartado se describe una de las brechas de datos personales más significativas de las que han sido notificadas al Consejo durante el primer semestre de 2023. Su relevancia no se limita exclusivamente al impacto de la misma; también al hecho de que ésta pueda producirse con cierta facilidad en otros organismos y por tanto representa una oportunidad para aportar recomendaciones de aplicación general y evitar así que la misma se reproduzca.

Resumen de la brecha

Durante el fin de semana, se produjo el robo de un número significativo de equipos informáticos en un centro público. Las cámaras de seguridad captaron la intrusión pero el sistema de alarma no se activó.

Tras investigar los hechos, se descubrió que los equipos contenían una gran cantidad de datos personales, algunos de los cuales pertenecían a categorías especiales de datos personales definidas en el artículo 9 RGPD. Aunque estos datos estaban seudonimizados, surgieron dudas sobre el posible riesgo de reidentificación de personas concretas. Inmediatamente después de detectar el robo, se presentó una denuncia ante la Policía Nacional y se informó al centro de seguridad TIC para desactivar el acceso relacionado con dichos dispositivos. Sin embargo, no fue posible desactivar algunos de los equipos pertenecientes a personal de empresas externas.

El Delegado de Protección de Datos (DPD) de la entidad fue informado rápidamente y se notificó la brecha a la autoridad de control. El responsable del tratamiento realizó un análisis de riesgos de la brecha, y teniendo en cuenta la seudonimización de los datos y el hecho de que según la investigación realizada por la Policía, los presuntos autores eran delicuentes comunes, dicho responsable consideró como bajo el riesgo de re-identificación. Por tanto, se decidió no comunicar a los ciudadanos cuyos datos se encontraban en los dispositivos.

Recomendaciones: medidas correctivas y preventivas

Como consecuencia de lo anterior, se hacen una serie de recomendaciones sobre las posibles medidas a adoptar, divididas en dos categorías. Las primeras se orientan a limitar los efectos una vez que la brecha se ha producido. Las segundas, de mayor interés por su mayor impacto, se centran en disminuir la probabilidad de que la misma tenga lugar y en caso de que así sea, las consecuencias para los derechos y libertades de las personas físicas sean las mínimas posibles.

A) Medidas correctivas para limitar el impacto de la brecha

- Denunciar los hechos ante la Policía Nacional o la Guardia Civil.
- Informar al DPD y al Comité de Seguridad TIC del organismo.

- Proporcionar al DPD los datos necesarios con prontitud para evaluar el alcance del daño, teniendo en cuenta la información previa del inventario de sistemas.
- Notificar al centro de operaciones de seguridad correspondiente para que se desactiven de manera oportuna los permisos en los sistemas afectados.
- Notificar la brecha a la autoridad de control competente.
- Comunicar a los ciudadanos afectados, especialmente si existe un riesgo importante para sus datos personales (por ejemplo, acceso a números de cuenta corriente y datos de identificación). Esto les permitirá tomar medidas de protección. Aún sigue existiendo una inercia a no comunicar estas brechas a los ciudadanos, especialmente cuando afectan a un gran número de personas. Cualquier organización está sujeta a sufrir brechas de seguridad sin que eso implique necesariamente deficiencias en sus sistemas. Se recomienda a los órganos directivos de los organismos públicos advertir con prontitud a los ciudadanos sobre los posibles daños, considerándolo parte del servicio que se brinda a la ciudadanía.

B) Medidas relacionadas con la seguridad física

- Revisar y estudiar posibles mejoras en el servicio y sistema de seguridad física (vigilancia) de los centros, o implementarlos de inmediato si no existen. Asegurar la continuidad del servicio las 24 horas del día, los 7 días de la semana.
- Adoptar medidas básicas, como revisar la ubicación de los sensores de movimiento y cámaras, establecer horarios específicos de apertura y cierre de puertas según los horarios de trabajo y limitar la apertura y cierre de puertas interiores solo al personal autorizado.
- Instalar alarmas en las puertas de seguridad exteriores del edificio.
- Colocar cámaras de seguridad y sensores de movimiento en el área afectada.
- Asegurar que los equipos portátiles estén anclados a las mesas y cerrar con llave las salas vacías para evitar el acceso a los equipos.
- Etiquetar los equipos para su identificación.

C) Medidas relacionadas con la seguridad lógica

Estas medidas están dirigidas a la protección de los datos, especialmente los datos personales a los que se pueda acceder desde los dispositivos robados.

- Limitar al mínimo indispensable la información relacionada con el trabajo, especialmente en dispositivos portátiles y fácilmente sustraíbles (pendrives, tablets, smartphones, portátiles,etc.).
- Implementar medidas de protección, como la seudonimización de los datos.
- Cifrar el contenido de los datos almacenados en los dispositivos.

- Revisar y eliminar la información accidentalmente almacenada en los dispositivos.
- Evitar el almacenamiento accidental de credenciales de acceso.
- Establecer un sistema de credenciales robusto, que incluya contraseñas seguras con cambios periódicos y considerar la autenticación de doble factor.
- Establecer un sistema restrictivo de permisos y su revisión periódica, de manera que, en caso de acceder a los permisos de usuario, el riesgo sea limitado.

D) Medidas relacionadas con la gobernanza de la seguridad

- Definir qué tipo de información se puede almacenar en dispositivos fijos o portátiles.
- Establecer un sistema de gestión de incidentes que permita a los administradores de los sistemas desactivar rápidamente los sistemas o usuarios correspondientes en caso de robo.
- Contar con un sistema de inventario de equipos y una arquitectura de seguridad de los sistemas que permitan identificar los servicios e información afectados, así como el tipo y cantidad de datos personales involucrados.

Como puede observarse del compendio de medidas propuestas, y con carácter general se recomienda centrar los esfuerzos en labores preventivas que eviten que se produzca la brecha y en caso de que tenga lugar, se mitigen los posibles efectos adversos derivados de la misma, sin perjuicio de la necesidad de adoptar de forma ágil y eficiente medidas correctivas para reparar las consecuencias de la brecha de seguridad de datos personales.