Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

ORIENTACIONES PARA

COMUNICACIÓN A AFECTADOS DE BRECHAS DE DATOS PERSONALES

Objetivos

Garantizar la protección de las personas frente a los impactos potenciales de las brechas

Asegurar una respuesta responsable y transparente

Importancia de comunicar una Brecha a los afectados

1. Mitigación de Daños: Informar a los afectados les permite tomar medidas proactivas para mitigar los riesgos asociados al incidente generado por la brecha, como el fraude, la usurpación de identidad u otros daños potenciales.

2.Transparencia y Confianza: Comunicar de manera oportuna las brechas muestra un compromiso ético y responsable con la privacidad y seguridad de las personas. Al informar sobre qué pasos se están dando para resolver la situación y prevenir futuras incidencias, los organismos públicos transmiten confianza en la medida en que demuestran tener control sobre la situación.

3.Obligación Legal: El RGPD establece la obligación de comunicar a los afectados las brechas de seguridad de datos personales cuando estas puedan generar un riesgo alto para sus derechos y libertades. Su incumplimiento puede ser sancionado por el Consejo.

Cómo decidir si hay que comunicar la brecha

1. Asesoramiento del DPD: Aportará una perspectiva experta y especializada en protección de datos, asegurando la correcta evaluación del riesgo asociado a la brecha y la decisión sobre comunicarla o no.

2. Análisis de Riesgos: Realizar un análisis para determinar el nivel de riesgo asociado con la brecha, considerando la naturaleza de los datos afectados, el número de personas afectadas, y las circunstancias de la brecha. Habrá que valorar el perjuicio que la brecha puede causar a los afectados, como discriminación, fraude, daño a la reputación, sufrimiento psicológico, etc.

3. Evaluación sistemática: Para evaluar la severidad de la brecha y determinar si el riesgo es lo suficientemente alto como para requerir comunicación se recomienda utilizar herramientas o metodologías proporcionadas por autoridades competentes.

Puedes usar la herramienta **Comunica-Brecha** desarrollada por la AEPD, entre otras

www.ctpdandalucia.es/area-de-proteccion-de-datos/comunica-brecha-rgpd

Cuándo comunicar la brecha

1. Sin dilación: Debe realizarse sin retrasos indebidos. Es crucial actuar rápidamente, incluso si no se tienen todos los detalles sobre el incidente.

2. Evaluación Continua: En casos de ciberincidentes, donde el análisis forense puede demorar, es vital iniciar la comunicación basándose en la información disponible en ese momento y luego proporcionar actualizaciones conforme se disponga de más detalles.

Cómo se debe comunicar la brecha

1. Formato y contenido claro: La comunicación debe ser clara y directa, proporcionando información sobre el incidente, las medidas tomadas por la organización, las recomendaciones para que los afectados puedan protegerse y los datos de contacto para obtener más información.

2. Métodos de comunicación efectiva: Preferiblemente, la comunicación debe ser individualizada. En brechas con un gran número de afectados, se puede optar por publicaciones en sitios web o medios de comunicación, asegurando que el mensaje sea accesible y fácilmente comprensible para todos los afectados.

Consideraciones Adicionales

1. Enfoque orientado a la protección de datos: Se debe fomentar una cultura de protección de datos en la que la comunicación de las brechas sea considerada como una parte esencial de la gestión de la protección de datos personales, y no como un desprestigio para el organismo público. El riesgo cero, no existe.

2. Documentación y Justificación: Mantener un registro detallado de cualquier brecha de datos personales, los hechos relacionados con la misma y las medidas correctivas adoptadas, incluyendo la justificación de porqué se decidió o no notificar al Consejo así como comunicar a los afectados. En caso no justificar adecuadamente los motivos para no comunicar a los afectados, el Consejo podría ordenar hacerlo si aprecia alto riesgo para los derechos y libertades de las personas afectadas.

MODELO DE COMUNICACIÓN A AFECTADOS POR BRECHAS DE DATOS PERSONALES

nota: el modelo es una orientación al contenido de una comunicación eficiente y completa a los afectados por una brecha de datos personales. Dada la enorme casuística de brechas, resulta imposible proponer un modelo válido con carácter general.

No obstante, toda comunicación sí debe incluir los siguientes apartados:

- Descripción de la brecha
- Datos personales comprometidos
- Posibles consecuencias de la brecha
- Medidas de respuestas adoptadas
- Recomendaciones para su seguridad
- Contacto para información adicional
- Comunicación de actividades sospechosas

Comunicación de brecha de seguridad de datos personales

Le escribimos para informarle sobre un incidente de seguridad que implicó una brecha en la protección de sus datos personales. Este incidente ocurrió el [fecha exacta/aproximada], y estamos tomando todas las medidas a nuestro alcance para abordar y mitigar sus efectos.

1. Descripción de la brecha

[detalles en lenguaje claro y fácil de entender de la causa de la brecha**]**

2. Datos personales comprometidos

Datos comprometidos: [lista detallada de datos afectados, p.ej., nombre, dirección, etc.]. Estos datos estaban [indicar si estaban cifrados, seudonimizados o protegidos de alguna otra forma].

3. Posibles consecuencias de la brecha

[consecuencias específicas**]** (ejemplos:)

La brecha podría exponerle a riesgos como fraude o suplantación de identidad. Por ejemplo, podría haber intentos de transacciones fraudulentas con su información.

4. Medidas de respuesta adoptadas

[medidas específicas adoptadas o previstas**]** (ejemplos:)

Hemos adoptado las siguientes medidas para mitigar el impacto de la brecha:

- *Bloqueado el acceso no autorizado*

- *Estamos colaborando con expertos en seguridad para investigar y solucionar la brecha.*

5. Recomendaciones para su seguridad

[según el caso, las medidas recomendadas] (ejemplos:)

- *Revise sus cuentas y movimientos bancarios.*
- *Evite responder a solicitudes sospechosas de información.*
- *No haga clic en enlaces de fuentes desconocidas.*

6. Contacto para información adicional

Para obtener más información o si tiene alguna pregunta, puede ponerse en contacto con nuestro Delegado de Protección de Datos a través de [nombre, datos de contacto:correo electrónico/teléfono]

7. Comunicación de actividades sospechosas

Si detecta cualquier anomalía relacionada con sus datos, por favor contáctenos inmediatamente al [correo electrónico/teléfono].

[despedida]

[Nombre del Responsable del tratamiento]

[Teléfono] / [Correo electrónico de contacto]