GUÍA PARA REGISTRAR Y REPORTAR VULNERACIONES DE DATOS PERSONALES EN EL INSTITUTO MEXICANO DEL SEGURO SOCIAL

I. OBJETO

En términos de los artículos 37, 38, 39, 40 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), se emite la presente guía, que tiene como finalidad desarrollar las instrucciones y actividades para que las unidades administrativas del Instituto Mexicano del Seguro Social (IMSS) identifiquen y registren, adecuadamente, las vulneraciones que ocurran a la seguridad de los datos personales que tratan en sus actividades cotidianas y resguardan en sus archivos físicos y electrónicos, en cualquier fase del tratamiento de datos personales.

II. Vulneraciones a la seguridad de datos personales.

Debe entenderse por vulneraciones de datos personales a *"la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada." (Andrés Velázquez Olavarrieta, Diccionario de Protección de Datos Personales)*

En este sentido la LGPDPPSO, señala que por vulneraciones de seguridad debe entenderse, en cualquier fase del tratamiento de datos, al menos, las siguientes:

a) La pérdida o destrucción no autorizada;
b) El robo, extravío o copia no autorizada;
c) El uso, acceso o tratamiento no autorizado, o
d) El daño, la alteración o modificación no autorizada.

En caso de ocurrir una vulneración de seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita (artículo 37).

III. Instrucciones para el registro y reporte de vulneraciones

La unidad administrativa deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Por lo que la **Bitácora de Registro de Vulneraciones (A)** que se adjunta al presente atiende en sus términos lo establecido en el artículo 39 de la LGPDPPSO, que deberá ser implementado y conservado por las unidades administrativas para el registro histórico de las vulneraciones que se presenten a lo largo del tiempo.

Además, si la vulneración tiene el riesgo de repercutir significativamente en los derechos patrimoniales o morales de sus titulares de los datos personales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos (artículo 40).

En atención a ello, la unidad administrativa deberá informar al titular al menos lo siguiente:

a) La naturaleza del incidente;
b) Los datos personales comprometidos;
c) Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger
d) sus intereses;
e) Las acciones correctivas realizadas de forma inmediata, y
f) Los medios donde puede obtener más información al respecto.

Ahora bien, cuando se presente alguna de las situaciones enunciadas, con el propósito de asegurar un control adecuado en el momento que ocurren las vulneraciones y garantizar la no repetición de éstas, es necesario implementar las siguientes acciones:

1. La persona que observe o conozca sobre una vulneración de datos personales, deberá informar inmediatamente a la persona responsable de seguridad de datos personales (RESPONSABLE) designada en el área de su adscripción.
2. Por su parte, la persona RESPONSABLE deberá informar inmediatamente sobre la vulneración a la persona titular del área de su adscripción y entablar contacto con la Unidad de Transparencia, para informar el hecho y que ésta disponga lo conducente para orientar y acompañar en las gestiones que deban documentarse, las cuales deben realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.
3. La persona RESPONSABLE coordinará las acciones preventivas que se estimen convenientes al interior del área de su adscripción para asegurar el cese inmediato de la vulneración.
4. Una vez implementadas las acciones preventivas, se deberá documentar, a través de los formatos señalados.

5. Identificada y registrada esta información, se deberán implementar y planear las acciones correctivas de corto plazo, en coordinación con la Unidad de Transparencia y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes.
6. En caso de que se deba informar a los titulares o al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales, la Unidad de Transparencia realizará los requerimientos internos necesarios para recabar información suficiente y emitirá las comunicaciones correspondientes.
7. Al final de este proceso, deberá concluirse la información de la **Bitácora de Registro de Vulneraciones (B).**

Es importante señalar que la versión original de los documentos generados se firmará por la persona RESPONSABLE y permanecerá bajo resguardo del área involucrada. Además, se remitirá un ejemplar en copia simple a la Unidad de Transparencia para el seguimiento respectivo.

Bitácora de Registro de Vulneraciones (A)

Área:		
Vulneración de datos personales ocurrida el día:		
Rubro	**Información**	
Tratamiento(s) de datos personales afectado(s) [1]	Nombre	
	Clave	
Nombre y cargo de quien reporta la vulneración dentro del área[2]		
Fecha y hora aproximada de la vulneración[3]		
Tipo de vulneración no autorizada[4]	Pérdida o destrucción	
	Robo, extravío o copia	
	Uso, acceso o tratamiento	
	Daño, alteración o modificación	

1 Tratamiento(s) de datos personales afectado(s). El nombre y la clave de identificación registradas en el Inventario de Tratamientos de Datos Personales.
2 Nombre y cargo de quien reporta la vulneración dentro del área. Es decir, de la persona que tuvo conocimiento por primera vez.
3 Fecha y hora aproximada de la vulneración. En caso de que se requiera, se deberá corroborar esta información con el área correspondiente.
4 Tipo de vulneración. Precisar si se trata de pérdida o destrucción; robo, extravío o copia; uso, acceso o tratamiento; o, daño, alteración o modificación. Siempre que esos supuestos sean no autorizados.

Bitácora de Registro de Vulneraciones (B)

Área:	
Vulneración de datos personales ocurrida el día:	
Rubro	Información
Motivos (posibles o identificados) de la vulneración[5]:	
Acciones preventivas realizadas por el área para cesar la vulneración[6]	
Fecha y hora en que se hizo del conocimiento a la Unidad de Transparencia[7]	
Nombre y cargo del responsable de seguridad que informó sobre la vulneración a la Unidad de Transparencia[8]	

5 Motivos (posibles o identificados) de la vulneración. El motivo se relaciona con identificar las acciones u omisiones de cualquier persona -incluso ajena a la institución- que pudieran haber provocado la vulneración y sea posible distinguirlas en ese momento.
6 Acciones preventivas realizadas por el área responsable. Aquellas coordinadas por la persona RESPONSABLE al interior del área de su adscripción para cesar la vulneración inmediatamente, así como las áreas involucradas en su consecución.
7 Fecha y hora aproximada en que se hizo del conocimiento a la Unidad de Transparencia. La realizada en primera instancia por la persona RESPONSABLE. Para tener registro de ello, dicha comunicación podrá realizarse a través del correo electrónico a la cuenta institucional de la persona titular de la Unidad de Transparencia.
8 Nombre y cargo del responsable de seguridad que informó sobre la vulneración a la Unidad de Transparencia. La persona RESPONSABLE o, en su caso, aquella que informó a la Unidad de Transparencia.
9 Acciones correctivas implementadas y/o planeadas por las áreas competentes. Las implementadas definitivamente y/o planeadas en el corto plazo, así como las áreas involucradas en su consecución.

Acciones correctivas implementadas definitivamente y/o planeadas en el corto plazo[9]	Implementadas definitivamente	
	Planeadas a corto plazo	
Comentarios adicionales		
Firma de la persona responsable de seguridad de datos		