Guía para registrar y reportar vulneraciones de datos personales en el Instituto de Investigaciones Dr. José María Luis Mora

I. Objeto

En cumplimiento con 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. Su finalidad es desarrollar instrucciones y actividades para que las áreas administrativas del Instituto de Investigaciones Dr. José María Luis Mora identifiquen y registren adecuadamente las vulneraciones 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 dichos datos.

II. Vulneraciones a la seguridad de datos personales.

Se entiende por vulneraciones de datos personales la materialización de amenazas que pueden centrarse en la pérdida o destrucción no autorizada de los datos personales en posesión de personas físicas o morales que los gestionan. También incluye el robo, extravío o copia no autorizada de dichos datos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada de los mismos. En este sentido, la presente LGPDPPSO establece que las vulneraciones de seguridad en cualquier fase del tratamiento de datos personales deben comprender, al menos, los siguientes aspectos:

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 que la originaron e implementar en su plan de trabajo las acciones preventivas y correctivas necesarias para adecuar las medidas de seguridad y el tratamiento de los datos personales, con el fin 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 describan la naturaleza de la vulneración, la fecha en que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva. La Bitácora de Registro de Vulneraciones (A), que se adjunta al presente documento, cumple con lo establecido en el artículo 39 de la LGPDPPSO y deberá ser implementada y conservada por las áreas administrativas para el registro histórico de las vulneraciones que se presenten a lo largo del tiempo.

Si la vulneración tiene el riesgo de repercutir significativamente en los derechos patrimoniales o morales de los titulares de los datos personales, se deberá informar a los titulares tan pronto como se confirme la ocurrencia de la vulneración y el responsable haya comenzado a tomar las acciones necesarias para una revisión exhaustiva de la magnitud de la afectación. Esto permitirá 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 en que ocurren las vulneraciones y garantizar que no se repitan, es necesario implementar las siguientes acciones:

1. La persona servidora pública que observe o tenga conocimiento de una vulneración de datos personales deberá informar inmediatamente a su mando superior inmediato.
2. El mando superior deberá informar de inmediato sobre la vulneración a la Unidad de Transparencia, para que esta última tome las medidas adecuadas para orientar y acompañar en las gestiones que deban documentarse. Estas acciones deben realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.
3. La persona de mando superior adscrita al área administrativa afectada deberá coordinar las acciones preventivas que se estimen convenientes al interior de su área para asegurar el cese inmediato de la vulneración.
4. Una vez implementadas las acciones preventivas, se deberá documentar la situación utilizando los formatos señalados.
5. Identificada y registrada la información, se deberán planear e implementar las acciones correctivas a corto plazo en coordinación con la Unidad de Transparencia y las áreas competentes, para subsanar la vulneración y evitar futuros 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 finalizar este proceso, se deberá completar la información en la Bitácora de Registro de Vulneraciones (B).

Es importante señalar que la versión original de los documentos generados deberá ser firmada por la persona servidora pública correspondiente y permanecerá bajo resguardo del área involucrada. Además, se remitirá una copia simple a la Unidad de Transparencia para el seguimiento respectivo.

Bitácora de Registro de Vulneraciones (A)

Nombre del Área administrativa vulnerada:	
Vulneración de datos personales ocurrida el día:	

Campo	Información	
Nombre del tratamiento(s) de datos personales afectado(s)	*"El nombre y la clave de identificación registradas en el Inventario de Tratamientos de Datos Personales."*	
Nombre y cargo de quien reporta la vulneración dentro del área.	*"Es decir, de la persona que tuvo conocimiento por primera vez."*	
Fecha y hora aproximada de la vulneración.	*"En caso de que se requiera, se deberá corroborar esta información con el área correspondiente."*	
Tipo de vulneración no autorizada.	**Pérdida o destrucción**	*"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."*
	Robo, extravío o copia	*"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."*
	Uso, acceso o tratamiento	*"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."*
	Daño, alteración o modificación	*"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)

Nombre del Área administrativa vulnerada:		
Vulneración de datos personales ocurrida el día:		
Campo	**Información**	
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.*	
Acciones preventivas realizadas por el área para cesar la vulneración.	*Aquellas acciones para cesar la vulneración inmediatamente, así como las áreas involucradas en su consecución.*	
Fecha y hora en que se hizo del conocimiento a la Unidad de Transparencia	*La realizada en primera instancia por la persona servidora pública. 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.*	
Nombre y cargo del servidor público que informó sobre la vulneración a la Unidad de Transparencia.	*La persona servidora pública que informó a la Unidad de Transparencia.*	
Acciones correctivas implementadas definitivamente y/o planeadas en el corto plazo.	**Implementadas definitivamente**	*Las acciones implementadas definitivamente y/o planeadas en el corto plazo, así como las áreas involucradas en su consecución*
	Planeadas a corto plazo	*Las acciones implementadas definitivamente y/o planeadas en el corto plazo, así como las áreas involucradas en su consecución*
Comentarios adicionales		
Firma de la persona servidora pública		