INSTRUCTIVO PARA REGISTRAR Y REPORTAR VULNERACIONES DE DATOS PERSONALES

Instructivo para el registro y reporte de vulneraciones

Descripción breve

Este documento tiene como propósito desarrollar las instrucciones para que las áreas de los Sujetos Obligados identifiquen y registren, adecuadamente, las vulneraciones que ocurran a la seguridad de los datos personales.

DPDP
ITAIH

Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo

I. Propósito

El plan de trabajo en materia de protección de datos personales del Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo, contempla la elaboración de documentos que sean herramientas administrativas para garantizar las medidas de seguridad suficientes para la protección de los datos personales. En tal sentido se crea el Instructivo para el Registro y Reporte de Vulneraciones de Datos Personales. Dicho documento delineó dos objetivos fundamentales:

1. Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,
2. Consolidar y preservar los niveles de protección de los datos personales con mecanismos de monitoreo y revisión.

Una de las medidas de seguridad administrativas que se incluyó fue la BITÁCORA DE VULNERACIONES en términos de los artículos 56, 57, 58, 59 y 60 de la Ley Estatal de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo (LGPDPPSOEH).

Este documento tiene como propósito desarrollar las instrucciones para que las áreas de los Sujetos Obligados 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.

II. Vulneraciones a la seguridad de datos personales

Las vulneraciones a la seguridad de los datos personales pueden ocurrir en cualquier etapa del tratamiento (registro, uso, aprovechamiento, conservación, etcétera). En ese sentido, por vulneraciones se deben entender, por lo menos, las siguientes circunstancias respecto de datos personales (en particular), bases de datos y/o sistemas que los albergan (en general):

1. La pérdida o destrucción no autorizada;
2. El robo, extravío o copia no autorizada;
3. El uso, acceso o tratamiento no autorizado; o
4. El daño, la alteración o modificación no autorizada.

Cuando se presenta alguna de estas situaciones, existe la obligación de analizar las causas por las cuales se presentó una vulneración e implementar acciones preventivas y correctivas para evitar que la vulneración afecte a más titulares y/o se repita (artículo 59).
Además, si la vulneración tiene el riesgo de repercutir significativamente en los derechos patrimoniales o morales de sus titulares (por ejemplo, las sucedidas sobre datos sensibles), se debe informar sobre ésta, sin dilación alguna, a los titulares afectados y, según sea el caso, al organismo garante. Este aviso previene a los titulares para que puedan tomar las medidas correspondientes en la defensa de sus derechos (artículo 57).

Para garantizar la atención adecuada de cualquier vulneración de datos personales, es necesario que cada área cuente con su propia BITÁCORA DE VULNERACIONES (usando el modelo que se adjunta al presente documento) y siga las instrucciones que se desarrollan en el apartado siguiente.

La esencia de este documento es fungir como una directriz para actuar con responsabilidad y celeridad en términos de las disposiciones legales en materia de protección de datos personales.

III. Instrucciones para el registro y reporte de vulneraciones

Para reportar vulneraciones a la seguridad de datos personales, se cuenta con un modelo de bitácora (anexo al final de este documento) que deberá ser implementado y conservado por las áreas para el registro histórico de las vulneraciones que se presenten a lo largo del tiempo.

De conformidad con los parámetros de la propia LEPDPPSOEH, la bitácora debe contener, cuando menos, fecha del incidente, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva (artículo 56).

Cuando se presente alguna de las situaciones enunciadas en el apartado II, 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 su titular, 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 la BITÁCORA DE VULNERACIONES, la siguiente información:

   a) Tratamiento(s) de datos personales afectado(s). El nombre y la clave de identificación registradas en el Inventario de Tratamientos de Datos Personales.
   b) Nombre y cargo de quien reporta la vulneración dentro del área. Es decir, de la persona que tuvo conocimiento por primera vez.
   c) Fecha y hora aproximada de la vulneración. En caso de que se requiera, se deberá corroborar esta información con el área correspondiente.
   d) 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.
   e) 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.
   f) 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.
   g) Fecha y hora aproximada en que se hizo del conocimiento a la UT. 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 UT.
   h) Nombre y cargo del responsable de seguridad que informó sobre la vulneración a la UT. La persona RESPONSABLE o, en su caso, aquella que informó a la UT.

5. Identificada y registrada esta información, se deberán implementar y/o planear las acciones correctivas de corto plazo, en coordinación con la UT y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes.
6. En caso de que se deba informar a los titulares y/o al organismo garante sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales, la UT 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 VULNERACIONES, incluyendo la siguiente información:

   i) 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.

La versión original de la BITÁCORA DE VULNERACIONES se firmará por la persona RESPONSABLE y permanecerá bajo resguardo del área involucrada. Además, se remitirá un ejemplar en copia simple a la DPDP para el seguimiento respectivo.

ANEXO. MODELO DE BITÁCORA DE VULNERACIONES DE DATOS PERSONALES

ÁREA:			
VULNERACIÓN DE DATOS PERSONALES OCURRIDA EL DÍA:			
RUBRO	INFORMACIÓN		
TRATAMIENTO(S) DE DATOS PERSONALES AFECTADO(S)	Nombre		
	Clave		
NOMBRE Y CARGO DE QUIEN REPORTA LA VULNERACIÓN DENTRO DEL ÁREA			
FECHA Y HORA APROXIMADA DE LA VULNERACIÓN			
TIPO DE VULNERACIÓN NO AUTORIZADA	Pérdida o destrucción		
	Robo, extravío o copia		
	Uso, acceso o tratamiento		
	Daño, alteración o modificación		

ÁREA:		
VULNERACIÓN DE DATOS PERSONALES OCURRIDA EL DÍA:		
RUBRO	INFORMACIÓN	
MOTIVOS (POSIBLES O IDENTIFICADOS) DE LA VULNERACIÓN:		
ACCIONES PREVENTIVAS REALIZADAS POR EL ÁREA PARA CESAR LA VULNERACIÓN		
FECHA Y HORA EN QUE SE HIZO DEL CONOCIMIENTO A LA UT		
NOMBRE Y CARGO DEL RESPONSABLE DE SEGURIDAD QUE INFORMÓ SOBRE LA VULNERACIÓN A LA UT		
ACCIONES CORRECTIVAS IMPLEMENTADAS DEFINITIVAMENTE Y/O PLANEADAS EN EL CORTO PLAZO	Implementadas definitivamente	
	Planeadas a corto plazo	
COMENTARIOS ADICIONALES		
FIRMA DE LA PERSONA RESPONSABLE DE SEGURIDAD DE DATOS		