MOVIMIENTO CIUDADANO

GUÍA PARA EL USO DE LA BITACORA DE VULNERACIONES

CNTYAI
UNIDAD DE DATOS PERSONALES

REVISIÓN: ENERO DE 2022

INDICE

Presentación

El presente documento tiene como finalidad orientar al personal de Movimiento Ciudadano, que trata datos personales sobre el manejo de la bitácora de vulneraciones que exige el artículo 39 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Esto implica, que de haber una vulneración a los sistemas donde son resguardados los datos personales que por su actividad recolecta Movimiento Ciudadano, ésta debe quedar registrada en el ***formato de identificación de incidentes***, el cual forma parte de la bitácora de vulneraciones, así como también se deben tomar diversas medidas al respecto, ya que el artículo 40 de la LGPDPPSO, exige informar a los titulares afectados y al órgano garante correspondiente.

Importancia de la notificación de la vulneración

La notificación de vulneraciones de seguridad es considerada una medida de seguridad, por lo que la LGPDPPSO la considera una obligación del responsable del sistema de datos personales para que los titulares puedan tomar medidas para la protección de sus derechos morales y patrimoniales, por lo que es nuestra obligación notificarles en caso de que ésta suceda, se debe además notificar al INAI o al organismo garante correspondiente en un plazo no mayor a 72 horas una vez identificado el incidente.

Proceso de notificación de vulneraciones

La notificación de vulneraciones se debe realizar lo antes posible al jefe superior inmediato, con la información suficiente mediante correo electrónico o en persona.

IMPORTANTE: La Unidad de Protección de Datos Personales proveerá la asesoría y ayuda requerida.

Para la estructura nacional:

- Cada unidad administrativa responsable debe llevar una bitácora nacional.
- La Unidad de Datos Personales debe llevar una bitácora general.
- De ocurrir una vulneración, el responsable del sistema de datos personales debe registrarla en la bitácora nacional y notificar a la Unidad de Datos Personal para efecto de que ésta se inscriba en la bitácora general y se dé conocimiento de lo ocurrido a la Comisión Nacional de Transparencia y Acceso a la Información. Este órgano deberá notificar a los titulares de datos y al garante.

La notificación de vulneraciones al titular y al INAI o al organismo garante correspondiente se debe hacer cuando ya se tenga información concreta del incidente y cuando ya no exista exposición de los activos involucrados en la vulneración, esto debe ocurrir en un plazo máximo de 72 horas a partir de que la vulneración se confirme.

La notificación al titular debe ser directa, es decir, mediante correo electrónico, teléfono o en persona y con un contenido específico, el cual se verá en el apartado de informes de vulneración.

IMPORTANTE: Se puede optar por la notificación al titular a través de sitios web o medios de comunicación masivos, cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información de contacto.

La notificación al INAI o al organismo garante correspondiente deberá ser mediante escrito, cuyo contenido específico se verá en el apartado de informes de vulneración, el cual deberá presentarse en el domicilio del Instituto, o a través del medio habilitado para tal efecto.

Para las entidades federativas:

- Cada unidad de transparencia local debe realizar supervisiones constantes a las unidades administrativas y llevar una bitácora estatal en caso de ocurrir una vulneración, la unidad administrativa además de notificar a la unidad de transparencia local, deberá notificar a su superior en oficinas del nacional.
- La Unidad de Datos Personales debe llevar una bitácora general.
- De ocurrir una vulneración, ésta se debe de inscribir en la bitácora estatal y después notificar a la Unidad de Datos Personales para efecto de que se inscriba en la bitácora general; la Unidad de Transparencia Local deberá poner la entrada en la bitácora a consideración de la Comisión Estatal de Transparencia.
- La Comisión Estatal de Transparencia deberá notificar a los titulares de datos y al garante local.

IMPORTANTE: Si ocurrida una vulneración de seguridad, se identifica un posible delito, se debe dar parte al Ministerio Público.

Existen tres formatos de bitácora, las cuales cada una debe de reunir los requisitos mínimos señalados por la ley:

- **Bitácora Nacional**: Realizada por la unidad administrativa responsable del nacional. ANEXO 1

- **Bitácora Estatal:** Realizada por las entidades federativas, esta debe levantarse por el titular de la unidad de transparencia local. ANEXO 2

- **Bitácora General:** Realizada por la Unidad de Transparencia Nacional, en la que se concentra las vulneraciones ocurridas, esta residirá en la Unidad de Datos Personales. ANEXO 3

IMPORTANTE: Todos los datos solicitados en los formatos, deben ser llenados

Notificación de la vulneración de seguridad

Informes de vulneración al titular

La Ley mandata que se realice un informe de vulneración al titular debidamente fundado y motivado (ANEXO 4), el cual deberá contener al menos lo siguiente:

a) **La naturaleza del incidente:**
Explicación general de las circunstancias en torno a la vulneración ocurrida, en qué consistió, fecha y hora en que ocurrió. No incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

b) **Datos personales comprometidos:**
Descripción de la información involucrada en el incidente.

c) **Recomendaciones dirigidas a los titulares:**
El listado de acciones que puede realizar el titular para minimizar los efectos de la vulneración.

d) **Acciones correctivas realizadas de forma inmediata:**
Descripción general de las acciones implementadas para evitar que incidentes similares se repitan.

e) **Los medios donde puede obtener más información al respecto**
Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad.

f) **La descripción de las circunstancias generales en torno a la vulneración que ayude al titular a entender el impacto del incidente y sus posibles consecuencias**

Informes de vulneración al instituto

La Ley mandata que se realice un informe de vulneración debidamente fundado y motivado, el cual deberá contener al menos lo siguiente:

g) **La naturaleza del incidente:**
Explicación detallada de las circunstancias en torno a la vulneración ocurrida, en qué consistió, fecha y hora en que ocurrió, fecha y hora del inicio de la investigación. No incluir información que revele vulnerabilidades o fallas específicas en los sistemas.

h) **Datos personales comprometidos:**
Categorías y número aproximado de titulares afectados, los sistemas de tratamientos y datos personales comprometidos.

i) **La descripción de las posibles consecuencias de la vulneración**

j) **Recomendaciones dirigidas a los titulares:**
El listado de acciones que puede realizar el titular para minimizar los efectos de la vulneración.

k) **Acciones correctivas realizadas de forma inmediata:**
Descripción general de las acciones implementadas para evitar que incidentes similares se repitan.

l) **El medio puesto a disposición del titular para que pueda obtener más información al respecto.**
Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad.

m) **Información de contacto:**
Nombre completo del personal y sus datos de contacto, que proporcionará al instituto información adicional del incidente en caso de que se requiera.

IMPORTANTE: En el informe al órgano garante, además de lo anterior, se deberá justificar que las medidas que se tomaron para el resguardo antes de la vulneración, eran acordes a la Ley y a las mejores prácticas. ANEXO 5.

ANEXO 1

MOVIMIENTO CIUDADANO	**BITACORA NACIONAL DE VULNERACIONES**
	FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN DEL PERSONAL QUE DETECTA EL INCIDENTE				
UNIDAD RESPONSABLE:				
NOMBRE				
DIRECCIÓN				
CORREO ELECTRÓNICO				
TELÉFONO LOCAL		CELULAR		
INFORMACIÓN SOBRE EL INCIDENTE				
FECHA		HORA		
LUGAR DONDE SE DETECTÓ:				
TIPO DE SISTEMA DE TRATAMIENTO DE DATOS PERSONALES				
FÍSICO		ELECTRÓNICO		
NOMBRE DEL RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADO				
SE ENCUENTRAN INVOLUCRADOS DATOS PERSONALES				
SI		NO		
DATOS PERSONALES INVOLUCRADOS				
DESCRIPCIÓN DE LO SUCEDIDO ¿Cómo fue detectado?, ¿Que sucedió?, ¿Que lo causo?				

ANEXO 1

PARA SER LLENADO POR EL EQUIPO DE GESTIÓN DE INCIDENTES			
MENCIONAR SI EXISTE ALGÚN IMPACTO LEGAL O CONTRACTUAL POR EL INCIDENTE DE SEGURIDAD			
RESUMEN EJECUTIVO DEL INCIDENTE (Motivo, descripción de la vulneración y titulares afectados)			
RESUMEN TÉCNICO DEL INCIDENTE			
DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PERDIDA O EXTRAVIO		ESPIONAJE	
OTRO		INGENIERÍA SOCIAL	
ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA			
NOMBRE Y FIRMA			
RESPONSABLE DEL SISTEMA DE DATOS PERSONALES		RESPONSABLE UNIDAD DE DATOS PERSONALES	

ANEXO 2

MOVIMIENTO CIUDADANO	**BITACORA ESTATAL DE VULNERACIONES** **FORMATO DE IDENTIFICACIÓN DE INCIDENTES**

INFORMACIÓN DEL PERSONAL QUE DETECTA EL INCIDENTE			
UNIDAD RESPONSABLE:			
NOMBRE			
DIRECCIÓN			
CORREO ELECTRÓNICO			
TELÉFONO LOCAL		CELULAR	
INFORMACIÓN SOBRE EL INCIDENTE			
FECHA		HORA	
LUGAR DONDE SE ETECTÓ:			
TIPO DE SISTEMA DE TRATAMIENTO DE DATOS PERSONALES			
FÍSICO		ELECTRÓNICO	
NOMBRE DEL RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADO			
SE ENCUENTRAN INVOLUCRADOS DATOS PERSONALES			
SI		NO	
DATOS PERSONALES INVOLUCRADOS			
DESCRIPCIÓN DE LO SUCEDIDO ¿Cómo fue detectado?, ¿Que sucedió?, ¿Que lo causo?			

ANEXO 2

PARA SER LLENADO POR EL EQUIPO DE GESTIÓN DE INCIDENTES			
MENCIONAR SI EXISTE ALGÚN IMPACTO LEGAL O CONTRACTUAL POR EL INCIDENTE DE SEGURIDAD			
RESUMEN EJECUTIVO DEL INCIDENTE (Motivo, descripción de la vulneración y titulares afectados)			
RESUMEN TÉCNICO DEL INCIDENTE			
DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PERDIDA O EXTRAVIO		ESPIONAJE	
OTRO:		INGENIERÍA SOCIAL	
ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA			
NOMBRE Y FIRMA			
RESPONSABLE DEL SISTEMA EN EL ESTADO		COMISION DE TRANSPARENCIA LOCAL	

ANEXO 3

MOVIMIENTO CIUDADANO	**BITACORA GENERAL DE VULNERACIONES**
	FORMATO DE IDENTIFICACIÓN DE INCIDENTES
INFORMACIÓN DEL PERSONAL QUE DETECTA EL INCIDENTE	
UNIDAD O ENTIDAD RESPONSABLE:	
NOMBRE	
DIRECCIÓN	
CORREO ELECTRÓNICO	
TELÉFONO LOCAL	CELULAR
INFORMACIÓN SOBRE EL INCIDENTE	
FECHA	HORA
LUGAR DONDE SE DETECTÓ:	
TIPO DE SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	
FÍSICO	ELECTRÓNICO
NOMBRE DEL RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADO	
SE ENCUENTRAN INVOLUCRADOS DATOS PERSONALES	
SI	NO
DATOS PERSONALES INVOLUCRADOS	
DESCRIPCIÓN DE LO SUCEDIDO ¿Cómo fue detectado?, ¿Que sucedió?, ¿Que lo causo?	

ANEXO 3

PARA SER LLENADO POR EL EQUIPO DE GESTIÓN DE INCIDENTES			
MENCIONAR SI EXISTE ALGÚN IMPACTO LEGAL O CONTRACTUAL POR EL INCIDENTE DE SEGURIDAD			
RESUMEN EJECUTIVO DEL INCIDENTE (Motivo, descripción de la vulneración y titulares afectados)			
RESUMEN TÉCNICO DEL INCIDENTE			
DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PERDIDA O EXTRAVIO		ESPIONAJE	
OTRO:		INGENIERÍA SOCIAL	
ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA			
ACCIONES ADICIONALES Y NECESARIAS PARA SUBSANAR LA VULNERACIÓN			
NOMBRE Y FIRMA			
RESPONSABLE UNIDAD DE DATOS PERSONALES		COMISION NACIONAL DE TRANSPARENCIA	

ANEXO 4

FORMATO DE INFORME DE VULNERACIÓN AL TITULAR

Lugar y fecha

C. _____

En cumplimiento al mandato que establece el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, hago de su conocimiento que sus datos personales fueron vulnerados. Esto se debe a que en fecha … **(poner narrativa de los hechos que dan lugar a la vulneración)** de forma tal que sus datos personales **(listar los datos personales vulnerados)** fueron vulnerados al **… (establecer la forma en que se vulneraron los datos).**

Para tal efecto, se tomaron inicialmente las siguientes medidas: **(poner medidas iniciales)**; posteriormente, se decidió **(poner medidas posteriores si las hay)** y para efecto de registro, anexamos la entrada correspondiente de la bitácora de vulneraciones, que es el registro que por virtud del artículo 39 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

(la forma en que los hechos se relacionan con el marco jurídico).

Consideramos que la vulneración acontecida tiene como consecuencia para usted y sus derechos que **(explicar),** por lo que se recomienda **(poner las medidas que el titular puede adoptar para proteger sus intereses)**.

Usted puede obtener mayor información respecto a la vulnerabilidad detectada en **(mencionar el medios, referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas).**

Sin más, le reiteramos nuestro esfuerzo por proteger los datos personales que usted ha permitido sean resguardados y usados por nosotros.

_____

Presidente de la Comisión _____ de Transparencia

ANEXO 5

FORMATO DE INFORME DE VULNERACIÓN AL ORGANO GARANTE

Lugar y fecha

C. _____
(Puesto en el INAI)

En cumplimiento al mandato que establece el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, hago de su conocimiento que hubo una vulneración en nuestros sistemas de datos personales. Esto se debe a que en fecha … **(poner narrativa de los hechos que dan lugar a la vulneración dando una explicación detallada de lo ocurrido, en qué consistió, fecha y hora en que ocurrió, fecha y hora del inicio de la investigación. No incluir información que revele vulnerabilidades o fallas específicas en los sistemas)** de forma tal que los datos personales de **(número de personas, categorías y sistemas de datos personales comprometidos)** fueron vulnerados al **… (establecer la forma en que se vulneraron los datos).**

Para tal efecto, se tomaron inicialmente las siguientes medidas: **(poner medidas iniciales)**; posteriormente, se decidió **(poner medidas posteriores si las hay)** y para efecto de registro, anexamos la entrada correspondiente de la bitácora de vulneraciones, testando los datos personales.

(la forma en que los hechos se relacionan con el marco jurídico).

La vulneración acontecida tiene las siguientes consecuencias para los titulares y sus derechos **(explicar),** por lo que se recomiendo **(poner las medidas que el titular puede adoptar para proteger sus intereses)**.

El titular puede obtener mayor información respecto a la vulnerabilidad detectada en **(mencionar el medio, referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas).**

Consideramos que las medidas de resguardo antes de la vulneración eran acordes a la Ley y a las mejores prácticas **(explicar)**. Sin más, reiteramos nuestro esfuerzo por proteger los datos personales que nos han sido confiados.

En caso de requerir información relacionada con la vulneración detectada **(mencionar nombre completo del personal designado y sus datos de contacto para proporcionar información al instituto)** están a sus órdenes.

_____
Presidente de la Comisión _____ de Transparencia