GUÍA PARA EL USO DE LA BITÁCORA DE VULNERACIONES DE DATOS PERSONALES EN PODER DEL PARTIDO DEL TRABAJO

Presentación

El presente documento tiene como finalidad orientar a las personas que colaboran en el Partido del Trabajo y que tratan 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-.

En el supuesto de que haya una vulneración a los sistemas de bases de datos donde son resguardados los datos personales que por su actividad recolecta el Partido del Trabajo, ésta debe quedar registrada en el ***formato de identificación de incidentes***, el cual forma parte de la bitácora de vulneraciones, y 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 de la persona responsable del sistema de datos personales para que las personas titulares puedan tomar medidas para la protección de sus derechos morales y patrimoniales, por lo que es obligación del Partido del Trabajo notificarles en caso de que ésta suceda; además se debe notificar al INAI o al Órgano 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 de manera personal.

IMPORTANTE: El Oficial de Protección de Datos Personales proveerá la asesoría y ayuda requerida.

Para la estructura nacional:

- Cada órgano interno responsable debe llevar una bitácora nacional.
- El Oficial de Protección de Datos Personales debe llevar una bitácora general.
- De ocurrir una vulneración, la persona responsable del sistema de datos personales debe registrarla en la bitácora nacional y notificar al Oficial de Protección de Datos Personal para efecto de que ésta se inscriba en la bitácora general y se dé conocimiento de lo ocurrido al Comité de Transparencia. Este órgano colegiado deberá notificar a las personas titulares de datos y al Órgano Garante.

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

IMPORTANTE: Se puede optar por la notificación a la persona titular, a través de sitios web o medios de comunicación masiva, 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 Órgano Garante correspondiente deberá ser mediante escrito, cuyo contenido específico se abordará 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 los órganos internos responsables y llevar una bitácora estatal en caso de ocurrir una vulneración; el órgano interno responsable, además de notificar a la Unidad de Transparencia local, deberá notificar a La Comisión Ejecutiva Estatal y a la Comisionada Política o Comisionado Político Nacional adscrito.
- El Oficial de Protección de Datos Personales debe llevar una bitácora general.
- De ocurrir una vulneración, ésta se debe inscribir en la bitácora estatal y después notificar al Oficial de Protección de Datos Personales para efecto de que se inscriba en la bitácora general; la Unidad de Transparencia Local deberá asentar la entrada en la bitácora a consideración del Comité de Transparencia Estatal.
- El Comité de Transparencia Estatal deberá notificar a las personas titulares de datos y al Órgano 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 y cada una debe de reunir los requisitos mínimos señalados por la ley:

- **Bitácora Nacional**: Realizada por el órgano interno responsable de la Comisión Ejecutiva Nacional -ANEXO 1-

- **Bitácora Estatal y de la Ciudad de México:** Realizada por las entidades federativas, ésta debe levantarse por la persona 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 con el Oficial de Protección de Datos Personales. -ANEXO 3-

IMPORTANTE: Todos los datos solicitados en los formatos deben ser propocionados.

Notificación de la vulneración de seguridad

Informes de vulneración a la persona titular

La Ley mandata que se realice un informe de vulneración a la persona 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 las personas titulares:**
El listado de acciones que puede realizar la persona 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 las personas 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 al INAI debidamente fundado y motivado, el cual deberá contener al menos lo siguiente:

a) **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.

b) **Datos personales comprometidos:**
Categorías y número aproximado de personas titulares afectadas, los sistemas de tratamientos y datos personales comprometidos.

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

d) **Recomendaciones dirigidas a las personas titulares:**
El listado de acciones que puede realizar la persona titular para minimizar los efectos de la vulneración.

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

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

g) **Información de contacto:**
Nombre completo del colaborador 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 fueron acordes con la Ley y a las mejores prácticas. -ANEXO 5-.

TRANSITORIO. La presente Guía de vulneraciones de Datos Personales surtirá efectos legales internos inmediatamente después de ser aprobado por el Comité de Transparencia del Partido del Trabajo.

ANEXO 1

BITÁCORA NACIONAL DE VULNERACIONES

FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN DE LA PERSONA COLABORADORA QUE DETECTA EL INCIDENTE	
ÓRGANO INTERNO 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 DE LA PERSONA RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADA	
¿SE ENCUENTRAN INVOLUCRADOS DATOS PERSONALES?	
SI	NO
DATOS PERSONALES INVOLUCRADOS	
DESCRIPCIÓN DE LO SUCEDIDO ¿Cómo fue detectado?, ¿Qué sucedió?, ¿Qué lo causó?	

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 personas titulares afectadas)

RESUMEN TÉCNICO DEL INCIDENTE

DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PÉRDIDA O EXTRAVÍO		ESPIONAJE	
OTRO		INGENIERÍA SOCIAL	

ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA

NOMBRE Y FIRMA

RESPONSABLE DEL SISTEMA DE DATOS PERSONALES

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

COMITÉ DE TRANSPARENCIA

ANEXO 2

BITÁCORA DE VULNERACIONES ESTATAL O DE LA CIUDAD DE MÉXICO

FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN DE LA PERSONA COLABORADORA QUE DETECTA EL INCIDENTE	
ÓRGANO INTERNO 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 DE LA PERSONA RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADA	
¿SE ENCUENTRAN INVOLUCRADOS DATOS PERSONALES?	
SÍ	NO
DATOS PERSONALES INVOLUCRADOS	
DESCRIPCIÓN DE LO SUCEDIDO ¿Cómo fue detectado?, ¿Qué sucedió?, ¿Qué lo causó?	

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 personas titulares afectadas)

RESUMEN TÉCNICO DEL INCIDENTE

DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PÉRDIDA O EXTRAVÍO		ESPIONAJE	
OTRO:		INGENIERÍA SOCIAL	

ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA

NOMBRE Y FIRMA

RESPONSABLE DEL SISTEMA DE DATOS PERSONALES EN EL ESTADO O CDMX

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES EN EL ESTADO O CDMX

COMITÉ DE TRANSPARENCIA LOCAL

ANEXO 3

BITÁCORA GENERAL DE VULNERACIONES

FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN DE LA PERSONA COLABORADORA QUE DETECTA EL INCIDENTE	
ÓRGANO INTERNO NACIONAL U ÓRGANO INTERNO LOCAL Y 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?, ¿Qué sucedió?, ¿Qué lo causó?	

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 DELINCIDENTE			
DENEGACIÓN DEL SERVICIO		USO NO AUTORIZADO	
CÓDIGO MALICIOSO		ACCESO NO AUTORIZADO	
ROBO, PÉRDIDA O EXTRAVÍO		ESPIONAJE	
OTRO:		INGENIERÍA SOCIAL	

ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA

ACCIONES ADICIONALES Y NECESARIAS PARA SUBSANAR LA VULNERACIÓN

NOMBRE Y FIRMA

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

COMITÉ DE TRANSPARENCIA PT NACIONAL

ANEXO 4

FORMATO DE INFORME DE VULNERACIÓN A LA PERSONA TITULAR DE DATOS PERSONALES

Lugar y fecha

C. _____
P R E S E N T E

En cumplimiento con el 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 tal forma que sus datos personales correspondientes a **(listar los datos personales vulnerados)** fueron vulnerados al **… (establecer la forma en que se vulneraron los datos).**

Bajo dichas circunstancias, para contener el 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 el formato de Identificación de Incidentes correspondiente de la Bitácora de vulneraciones, que de conformidad con el artículo 39 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados es el registro que debe levantarse.

(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 la persona titular de los datos personales puede adoptar para proteger sus intereses)**.

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

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

C. ***
Presidencia del Comité de Transparencia

ANEXO 5

FORMATO DE INFORME DE VULNERACIÓN AL ÓRGANO GARANTE

Lugar y fecha

C. _____
(Puesto en el INAI)
P R E S E N T E

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 tal forma que los datos personales correspondientes a **(número de personas, categorías y sistemas de datos personales comprometidos)** fueron vulnerados al **… (establecer la forma en que se vulneraron los datos).**

Bajo dichas circunstancias, para contener el 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 el formato de Identificación de Incidentes correspondiente de la Bitácora de vulneraciones, que de conformidad con el artículo 39 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados es el registro que debe levantarse.

En ese contexto, inicialmente se tomaron las siguientes medidas: **(poner medidas iniciales)**; posteriormente se decidió **(poner medidas posteriores si las hay)** y para efecto de registro, anexamos el formato de Identificación de Incidentes 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 la persona titular de los datos personales y sus derechos **(explicar),** por lo que se recomiendo **(poner las medidas que la persona titular de los datos personales puede adoptar para proteger sus intereses)**.

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

Consideramos que las medidas de resguardo antes de la vulneración eran acordes con la Ley y a las mejores prácticas **(explicar)**.

Sin otro particular, 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 de la persona colaboradora designada y sus datos de contacto para proporcionar información al instituto)** están a sus órdenes.

C. ***
Presidencia del Comité de Transparencia