Suprema Corte
de Justicia de la Nación

Instructivo

Para registrar y reportar vulneraciones de datos personales

ABRIL 2026

I. Propósito

El Plan de Trabajo en materia de protección de datos personales fue aprobado por el Comité de Transparencia el 12 de noviembre de 2019, el cual encomendó su implementación a la entonces Unidad General de Transparencia y Sistematización de la Información Judicial, actualmente denominada Unidad de Transparencia de la Suprema Corte de Justicia de la Nación (UTSCJN). Dicho instrumento estableció 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 31, 32, 33 y 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Este documento tiene como propósito desarrollar las instrucciones para que las áreas de la Suprema Corte de Justicia de la Nación (SCJN) 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 31 de la LGPDPPSO).

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 34).

Para garantizar la atención adecuada de cualquier vulneración de datos personales, es necesario que cada área de la SCJN 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, la Unidad de Transparencia de la Suprema Corte de Justicia de la Nación (UTSCJN) diseñó 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 LGPDPPSO, la bitácora debe contener, cuando menos, fecha del incidente, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva (artículo 33).

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 vulnera-

ciones 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 UTSCJN, a través de 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 UTSCJN. 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 UTSCJN.

h) Nombre y cargo del responsable de seguridad que informó sobre la vulneración a la UTSCJN. La persona responsable o, en su caso, aquella que informó a la UTSCJN.

5. Identificada y registrada esta información, se deberán implementar y/o planear las acciones correctivas de corto plazo, en coordinación con la UTSCJN 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 UTSCJN realizar 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:

    a) 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 UTSCJN para el seguimiento respectivo.

Anexo. Modelo de Bitácora de Vulneraciones de Datos Personales

<table>
<tr><th colspan="4">Área</th></tr>
<tr><th colspan="4">VULNERACIÓN DE DATOS PERSONALES OCURRIDA EL DÍA</th></tr>
<tr><th>Rubro</th><th colspan="3">Información</th></tr>
<tr><td rowspan="2">TRATAMIENTO(S) DE DATOS PERSONALES AFECTADOS(S)</td><td>Nombre</td><td colspan="2"></td></tr>
<tr><td>Clave</td><td colspan="2"></td></tr>
<tr><td rowspan="4">TIPO DE VULNERACIÓN NO AUTORIZADA</td><td colspan="2">Pérdida o destrucción</td><td></td></tr>
<tr><td colspan="2">Robo, extravío o copia</td><td></td></tr>
<tr><td colspan="2">Uso, acceso o tratamiento</td><td></td></tr>
<tr><td colspan="2">Daño, alteración o modificación</td><td></td></tr>
</table>

Notificación de vulneración de seguridad	
Área u órgano	
Fecha y hora aproximada de la identificación de la vulneración	
Fecha y hora aproximada de ocurrida la vulneración	
Identificación del tratamiento de datos comprometido	
Tipo de vulneración ocurrida	
Descripción detallada de las circunstancias en torno a la vulneración ocurrida	
Categorías de titulares comprometidos	
Número aproximado de titulares comprometidos	
Datos personales comprometidos	
Acciones correctivas realizadas de forma inmediata	
Acciones correctivas realizadas de forma definitiva	
Posibles consecuencias de la vulneración ocurrida	
Cualquier información o documentación adicional	
Nombre de la persona servidora pública titular del área ode la dirección general responsable	Nombre de la persona servidora pública responsable, en este caso, del programa o plataforma dónde se manejan datos personales

Dudas o comentarios dirigirse a:

Unidad de Transparencia de la Suprema Corte de Justicia de la Nación

Dirección de Protección de Datos Personales

Correo electrónico: datospersonales@mail.scjn.gob.mx

Teléfono: 55-4113-1000 Ext.5817

Suprema Corte
de Justicia de la Nación