RECOMENDACIONES PARA LA ATENCIÓN DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS

Con fundamento en los artículos 36 al 41 de la Ley General de Protección de Protección de Datos Personales en Posesión de Sujetos Obligados y sus similares 38 al 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados Sujetos Obligados para el Estado de Quintana Roo (LPDPPSOQROO), los responsables del tratamiento están obligados a notificar las vulneraciones que ocurran en cualquier fase del tratamiento de datos, que afecten de forma significativa los derechos patrimoniales o morales de los titulares, así como a tomar medidas preventivas, correctivas y de mejora para evitar nuevas vulneraciones, para lo cual este Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo, emite las siguientes;

RECOMENDACIONES PARA LA ATENCIÓN INMEDIATA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS

PRIMERA. En términos del artículo 39 de la Ley Local en la materia, en caso de que ocurra alguna vulneración a la seguridad, el Responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo, las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la vulneración se repita.

Para tal efecto, el artículo 40 de la citada Ley, además de las que señalen las leyes respetivas y la normatividad aplicable, se consideran como vulneraciones de seguridad, en cualquier fase del tratamiento de datos al menos las siguientes:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

III. El uso, acceso o tratamiento no autorizado, o

IV. El daño, la alteración o modificación no autorizada.

SEGUNDA. Se recomienda conformar un Comité de Incidencias al interior del Sujeto Obligado, el cual debe estar integrado por:

I. El área responsable del Sistema de Tratamientos y colaboradores del Sistema (Ejemplo: Recursos Humanos responsable del Sistema de Nómina y el Área de Tecnologías de la Información, colaborador del Sistema encargado del soporte técnico).

II. Comité de Transparencia. Como máxima autoridad en materia de datos personales al interior de los Sujetos Obligados.

III. Área Jurídica. Para todos efectos legales que haya lugar.

IV. Órgano Interno de Control. Como el encargado del Acta de Hechos.

TERCERA. En términos del artículo 41 de la citada norma, el Responsable/Sujeto Obligado, deberá llevar una Bitácora de Vulnerabilidades a la seguridad ocurridas en la que se describa ésta, la fecha en la que ocurrió, el motivo de la misma y las acciones correctivas implementadas de forma inmediata y definitiva, para tal efecto, se pone a disposición el Formato 3S.4.02.SGSDP, descargable en la siguiente liga electrónica:

http://www.idaipqroo.org.mx/proteccion-de-datos-personales/sistema-de-gestion-de-seguridad/planeacion-y-diagnostico/

CUARTA. El responsable deberá informar sin dilación alguna al Titular y al Instituto, las vulneraciones de seguridad ocurridas que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos. Lo anterior, tal como lo señala el artículo 42 de la Ley en comento.

QUINTA. Se recomienda que en el caso de alguna vulneración a los datos personales, se realice la notificación en el momento adecuado y con la información suficiente, para evitar la exposición de los Sistemas de Tratamiento y de cualquier otro activo, a fin de que los titulares puedan estar protegidos.

En virtud de lo anterior, se recomienda que el responsable se formule las siguientes preguntas, para la adecuada notificación de vulneraciones:

I. **¿Cuándo notificar?**

a) En general, se recomienda notificar a los titulares en el menor tiempo posible;

b) Cuando ya se tenga información concreta del incidente; y

c) Cuando ya no exista exposición de los activos involucrados en la vulneración.

II. **¿Cómo notificar?**

El método recomendado de notificación es el directo con los titulares, es decir por teléfono, correo electrónico, correo postal, o en persona. En caso de que exista urgencia por contactar al titular, puede resultar oportuno utilizar más de un medio de contacto a la vez.

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

La notificación debe ser independiente y personalizada, y no debe incluir material o información no relacionada con el incidente de seguridad, ya que podría causar confusión.

III. **¿Quién debe notificar?**

El responsable del tratamiento de los datos personales, incluso si la vulneración ocurrió o involucró a un encargado.

IV. **¿A quién se debe notificar además del titular de los datos personales?**

Si derivado de la investigación de un incidente se identifica un posible delito, se debe dar parte al Ministerio Público competente.

Cuando un incidente resulte en una vulneración de seguridad, los responsables del sector público tienen la obligación de informar al Instituto mediante escrito presentado en el domicilio: Avenida Othón P. Blanco No. 66, Colonia Barrio Bravo, entre Cozumel y Josefa Ortiz de Domínguez, o bien a través de cualquier otro medio que se habilite para tal efecto, al menos lo siguiente:

a) La hora y fecha en que se identificó la vulneración;
b) La hora y fecha en que inició la investigación sobre la vulneración;
c) La naturaleza de la vulneración ocurrida;
d) La descripción detallada de cómo ocurrió la vulneración;
e) Los tipos de datos personales comprometidos y el número aproximado de titulares afectados;
f) Los sistemas de tratamiento comprometidos;
g) Las acciones correctivas realizadas de forma inmediata;

h) La descripción de las posibles consecuencias de la vulneración ocurrida;
i) Las recomendaciones dirigidas al titular;
j) El medio puesto a disposición del titular para que obtenga mayor información sobre la vulneración y cómo proteger sus datos personales;
k) El nombre completo de la o las personas designadas para proporcionar mayor información al IDAIPQROO.
l) Cualquier otra información o documentación que considere conveniente hacer del conocimiento del Instituto.

V. ¿Qué se debe notificar a los titulares?

El contenido de una notificación a los titulares puede variar dependiendo de la vulneración ocurrida; sin embargo, la información que proporcione el responsable debe servir para que el titular entienda el incidente y pueda prevenir una mayor afectación, la notificación debe considerar al menos:

a) **La Naturaleza del Incidente**. Descripción de la vulneración: Se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, así como el periodo en el que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

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

c) **Recomendaciones a los titulares acerca de las medidas que éste pueda adoptar.** El listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.

d) **Acciones correctivas realizadas de forma inmediata o de mitigación**: Una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.

e) **Los medios donde pueden obtener más información al respecto**. Información de contacto; datos de las áreas designadas, mesas de servicio o del personal de la organización que puede atender dudas y proporcionar información adicional del incidente.

f) **Fuentes de información adicional**: Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad, en su caso.

Asimismo, los responsables del sector público deberán notificar sin dilación alguna al IDAIPQROO, las vulneraciones de seguridad, a partir de que se confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

ACCIONES A ADOPTAR POR PARTE DEL IDAIPQROO ANTE LA NOTIFICACIÓN DE UNA VULNERACIÓN A LA SEGURIDAD DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

SEXTA. De conformidad con el artículo 45 de la Ley de la materia, una vez recibida la notificación de vulneración por parte del responsable, el Instituto deberá realizar las investigaciones previas a que haya lugar con la finalidad de allegarse de elementos que le permitan en su caso, iniciar el procedimiento de verificación, de conformidad al artículo 137 del citado ordenamiento que señala de manera literal lo siguiente:

Artículo 137. *La verificación podrá iniciarse:*

I. *De oficio cuando el Instituto cuente con indicios que le hagan presumir de manera fundada y motivada la existencia de violaciones a la presente Ley y demás normatividad que resulte aplicable;*
II. *Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable, o*
III. *Por denuncia de cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.*

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma.

Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

La verificación no procederá en los supuestos de procedencia del recurso de revisión previsto en la presente Ley.