De conformidad a los artículos 36 a 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 tomar medidas preventivas, correctivas y de mejora para evitar nuevas vulneraciones.

En razón del artículo 40 de la Ley Local en la materia, además de las que señalen las leyes respetivas y la normatividad aplicable, se consideran como vulnerables de seguridad, en cualquier fase del tratamiento de datos al menos las siguientes:

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.

De manera adicional, los responsables de la LPDPPSOQROO deben notificar las vulneraciones al Instituto, por consiguiente, el IDAIPQROO pone a disposición las siguientes recomendaciones para la notificación de vulnerabilidades. Lo anterior de manera homóloga y armónica a las “Recomendaciones para el manejo de incidentes de Seguridad de Datos Personales”, emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

En este sentido, 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.

A continuación, se presentan las preguntas que un responsable tiene que hacerse para la adecuada notificación de vulneraciones:

1. **¿Cuándo notificar?**
2. En general, se recomienda notificar a los titulares en el menor tiempo posible;
3. Cuando ya se tenga información concreta del incidente y
4. Cuando ya no exista exposición de los activos involucrados en la vulneración.
5. **¿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.

1. **¿Quién debe notificar?**

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

1. **¿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.

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.

1. **¿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**:

1. 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.
2. Datos personales involucrados: Una descripción de la información involucrada en el incidente.
3. Recomendaciones a los titulares: El listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.
4. Acciones correctivas o de mitigación: Una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.
5. 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.
6. 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.

Los responsables del sector público deberán notificar al titular y al IDAIPQROO, las vulneraciones de seguridad dentro **de un plazo máximo de setenta y dos horas**, 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. Dicho plazo comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.