zegarra & schipper
abogados consultores

INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

La falta de medidas de seguridad adecuadas y suficientes durante el tratamiento de datos personales puede provocar la exposición a adulteración, pérdida, consulta, uso o acceso no autorizado a los datos personales, situaciones que son denominadas como incidentes de seguridad.

A continuación, se desarrollan los aspectos más relevantes sobre los incidentes de seguridad y su regulación en la Ley 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su Reglamento.

1. ¿Qué es un incidente de seguridad?

La Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales (en adelante, la "Directiva")[1] ha definido al incidente de seguridad como todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas (p. 30), es decir, el tratamiento no autorizado del banco de datos personales.

2. ¿Qué tratamiento le ha dado la vigente normativa de protección de datos personales?

La ocurrencia de incidentes de seguridad configuran infracciones administartivas que se encuentran tipificadas en la normativa de protección de datos personales

Al respecto, la LPDP establece como una obligación del titular del banco de datos personales como del encargado de su tratamiento, el adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales (principio de seguridad), las cuales deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate (art. 9 y 16 de la LPDP).

El Decreto Supremo N° 003-2013-JUS, Reglamento de la LPDP, (en adelante, el RLPDP) ha regulado los incidentes de seguridad como infracciones en el tratamiento de datos personales de la siguiente manera:

- **Infracción leve:** por incumplir las medidas de seguridad exigidas por la normativa aplicable al tratar datos personales (inciso a del numeral 1 del art. 132 del RLPDP).

- **Infracción grave:**
  - Por realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad impuestas (inciso c del numeral 2 del art. 132 del RLPDP).
  - Por incumplir la obligación de confidencialidad establecida en el artículo 17 de la LPDP (inciso g del numeral 2 del art. 132 del RLPDP).

Finalmente, en la Directiva se ha señalado que los titulares o encargados del banco de datos personales deben coordinar las acciones requeridas para analizar y responder a los incidentes presentados; así como, efectuar el registro de los mismos (literal b del ítem 1.4.3).

[1] Véase en: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf.

3. ¿Cómo evitar los incidentes de seguridad?

Aquellos que realicen tratamiento de datos personales, a fin de evitar los incientes de seguridad, deben adoptar las medidas técnicas, organizativas y legales que garanticen la seguridad y eviten la alteración, pérdida, tratamiento o acceso no autorizado de los datos personales (art. 9 y 16 de la LPDP).

4. Acciones a realizar ante la ocurrencia de un incidente de seguridad

En la Directiva de Seguridad de la Información se establecen medidas se seguridad organizativas y técnica relacionadas a los incidentes de seguridad a implementarse de forma opcional u obligatoria dependiendo de la categoría de tratamiento de datos personales. Las mencionadas medidas de seguridad son las siguientes:

- Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales (ítem 2.1.10 del numeral 2.1 de la Directiva).

- El titular del banco de datos personales debe informar al titular de los mismos sobre los incidentes de tratamiento no autorizado del banco de datos, que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho (numeral 2.3.4.2 de la Directiva). Ni la LPDP ni el RLPDP, han previsto la obligación legal de comunicar a la ANPDP los incidentes de seguridad.

- Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales (ítem 2.3.4.9 de la Directiva).

- El encargado del banco de datos personales o quién sea designado por el titular del banco o datos personales deberá coordinar las acciones requeridas para analizar y responder en forma rápida y efectiva a los incidentes de seguridad presentados (numeral 2.3.5.6 de la Directiva).

5. Sobre la comunicación de los incidentes de seguridad y la comunicación que debe incluirse

De acuerdo con la Directiva de Seguridad emitida por la ANPDP, el titular o encargado del banco de datos personales debe informar al titular de datos personales, los incidentes que pudiesen afectar significativamente sus derechos patrimoniales o morales (p.29).

El titular del banco de datos debe incluir como mínimo la siguiente información en las comunicaciones:

a) Naturaleza del incidente.
b) Datos personales comprometidos.
c) Recomendaciones al titular de datos personales.
d) Medidas correctivas implementadas.

6. Información que debe incluirse en el registro de los incidentes de seguridad

Al registrar los incidentes de seguridad, el titular del banco de datos debe incluir como mínimo la siguiente información:

a) Fecha y hora del incidente.

b) Nombre de la persona que lo reporta.
c) Naturaleza del incidente.
d) Datos personales comprometidos.
e) Nombres de las personas involucradas en la resolución del incidente.
f) Consecuencias del incidente.
g) Medidas correctivas implementadas.
h) Recomendaciones para el titular de datos personales, de ser el caso.
i) Recuperación de datos.
j) En caso de haber realizado la recuperación de datos, se debe registrar:
- Nombre de la persona que realizó la recuperación.
- Descripción y fehca de los datos restaurados.
- Descripción de los datos restaurados en forma manual, de ser el caso.

7. Opiniones de la ANPDP relacionadas a los incidentes de seguridad

La ANPDP se ha pronunciado respecto a los incidentes de seguridad ocurridos durante el tratamiento de datos personales de la siguiente manera:

- **Opinión consultiva N° 024-2021-JUS/DGTAIPD:** Es posible cumplir las medidas de seguridad con criterios o protocolos distintos pero igualmente eficientes a los de la Directiva de Seguridad.

- **Informe N° 013-2018-DFI-VARS:** Los ciberataques no son considerados una causal de fuerza mayor, pues las medidas de seguridad deben estar orientadas a impedir la revelación y/o difusión de información de carácter personal sin consentimiento también en estos casos. Por ello, no se exime de sanción al titular del banco de datos personales en tal situación.

8. Posibles contingencias

La detección de incidentes de seguridad puede originar el inicio de un procedimiento administrativo sancionador, que podría devenir en la imposición de una multa desde 0.5 UIT hasta 50 UIT, dependiendo de la gravedad.

9. Comentario

El conocimiento respecto a los incidentes de seguridad contribuye a que las entidades o empresas que realizan tratamiento de datos personales adopten las medidas de seguridad adecuadas y suficientes para prevenirlos; así como, para tener en cuenta qué acciones deben realizar cuando se está ante la ocurrencia de un incidente de seguridad, con el fin de reducir el impacto en los derechos de los titulares de los datos personales.