JCDecaux

Procedimiento aplicable a la VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

JCDecaux – Top Media

PANAMÁ

I- OBJETIVO

- La Ley 81 de 26 de marzo de 2019 sobre protección de datos personales (en adelante "Ley 81") y el Decreto Ejecutivo 285 de 28 de mayo de 2021 que reglamenta la Ley 81 (en adelante "Reglamento Ley 81"), obligan a los responsables del tratamiento de datos personales a notificar las violaciones a la seguridad de los datos personales.

- Asegurar la seguridad de los datos personales requiere la implementación de medidas técnicas y organizacionales.

- Este procedimiento describe los diversos pasos a seguir, así como las partes potencialmente involucradas. Define las reglas a seguir para cumplir con la obligación de notificar a la autoridad de control, así como a los titulares afectados, en caso de violaciones a la seguridad de los datos personales.

II- ALCANCE

¿Qué es una violación a la seguridad de los datos personales?

- La Ley 81 define el Principio de Seguridad de los Datos (Art. 2.5) como "*los responsables del tratamiento de los datos personales deberán adoptar medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos bajo su custodia, principalmente cuando se trate de datos considerados sensibles, e informar al titular, lo más pronto posible, cuando los datos hayan sido sustraídos sin autorización o haya indicios suficientes de que su seguridad ha sido vulnerada*".

- El Reglamento Ley 81 define una violación a la seguridad de los datos personales (Art. 4.12) como "*Toda infracción a la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*"; y se refiere nuevamente a una violación de seguridad (Art. 37) como "*… cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, aun cuando ocurra de manera accidental, en cualquier fase del tratamiento y que represente un riesgo para la protección de los datos personales, …*".

- Estas definiciones abarcan:
  - Toda infracción a la seguridad;
  - Que ocasione la sustracción, destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma;
  - O la comunicación o acceso no autorizados a dichos datos.

- Por lo tanto, la violación puede:
  - Resultar de una acción maliciosa o de un simple error;
  - Ser atribuible a un tercero (por ejemplo, intrusión en la base de datos de un cliente) o a un miembro de JCDecaux (por ejemplo, recipiente erróneo de un e-mail dirigido a un cliente).

III- RESUMEN DE PASOS A SEGUIR

① Poner en marcha medidas apropiadas dirigidas a prevenir violaciones a la seguridad de los datos personales.

② Siguiendo la ocurrencia de una violación a la seguridad de los datos personales, identificarla y confirmarla.

③ Una vez que la violación haya sido identificada y confirmada, evaluar el nivel de riesgo que ésta puede suponer.

④ Implementar un plan de acción correctivo.

⑤ Notificar la violación a la autoridad de control (la Autoridad Nacional de Transparencia y Acceso a la Información - ANTAI) y a los titulares afectados.

⑥ Documentar toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento.

3.1 Poner en marcha medidas apropiadas dirigidas a prevenir violaciones a la seguridad de los datos personales

Responsables: Departamento de TI, Departamento de RRHH, Departamento Legal, todos los empleados

► **Medidas apropiadas deben ser implementadas** para prevenir, tan seguido como sea posible / en la mayor medida posible, cualquier violación a la seguridad de los datos personales y, en caso de ocurrencia de dicha violación, para hacer los datos ininteligibles para cualquier persona que no esté autorizada para acceder a dichos datos. Estas medidas son de naturaleza técnica y organizacional.

► Las medidas a ser tomadas **a nivel técnico** pueden incluir, en particular:
- La puesta en marcha por el Departamento de Seguridad de la información del Grupo, de una política de seguridad compuesta por la Política de Seguridad de TI;
- El cifrado de datos, siempre que la clave de cifrado no se haya visto comprometida;
- *Hashing*, considerando que el valor *hash* ha sido calculado usando una función *hash* estándar con una llave criptográfica. La llave debe ser generada de tal manera que ésta no pueda ser encontrada o comprometida.

► Las medidas a ser tomadas **a nivel organizacional** pueden incluir, en particular:
- Campañas operativas de concientización / capacitación para el personal;
- Crear y mantener vigente una "Política de uso de TI";
- Gestión del acceso físico (a través de la introducción de tarjetas, dispositivos de videovigilancia, etc.).

► La **ANTAI**, por sí o a través de la Dirección Nacional de Ciberseguridad de la Autoridad Nacional para la Innovación Gubernamental (AIG), difundirá información sobre higiene cibernética, específicamente sobre los Controles de Seguridad en Internet (CIS), un estándar aceptado a nivel mundial; según sea necesario, también podrá proporcionar capacitación a los miembros del sector privado. La Dirección Nacional de Ciberseguridad de la AIG también dirigirá la divulgación para difundir y fomentar el uso de normas y directrices básicas para la ciberseguridad. A través de la Dirección Nacional de Ciberseguridad de la AIG, las entidades del sector privado podrán comunicarse con otras entidades del sector privado sobre la inteligencia cibernética y el intercambio de información sobre amenazas.

3.2 Siguiendo la ocurrencia de una violación a la seguridad de los datos personales, identificarla y confirmarla

Responsables: Departamento de TI, el Departamento en cuestión, el proveedor de servicios de TI

- Existen **diversas formas en las cuales una potencial violación a la seguridad de los datos personales puede ser identificada y confirmada**:
  - Por la estructura responsable de proveer soporte a los usuarios, al informar de un problema técnico, un problema de hardware o la pérdida o robo de equipo. El empleado que identifique el problema contactará al área de Soporte Técnico e Infraestructura quien proporcionará el soporte de primer nivel de acuerdo al tipo de incidente reportado. El área de Soporte Técnico e Infraestructura alertará al Director de TI cuando ocurra un incidente de seguridad que cae fuera de su competencia.
  - Por el Departamento en cuestión, al reportar un incidente operativo, por ejemplo, que involucre una aplicación. El Departamento en cuestión alertará al responsable de TI encargado de la aplicación y este último será responsable de llevar a cabo una investigación del asunto.
    Por seguridad de TI vía comentarios automatizados sobre encuentros con amenazas o información de fuentes externas (por ejemplo, blogger, otros). El área de Soporte Técnico e Infraestructura confirmará el incidente, evaluará su severidad y reportará a las instancias adecuadas para seguimiento y solución.
- Ante la identificación y para evaluar el riesgo, las violaciones a la seguridad de datos personales pueden **ser clasificadas en tres categorías**, una misma violación puede clasificarse en más de una categoría:
  - Violación de la confidencialidad: revelación no autorizada o accidental de o acceso a datos personales;
  - Violación de la disponibilidad: pérdida o acceso accidental o no autorizado a o destrucción de datos personales;
  - Violación de la integridad: alteración accidental o no autorizada de datos personales.

- **Serán llevadas a cabo investigaciones** para asegurar la veracidad de la información suministrada en la alerta, y para obtener información confirmando, con un grado razonable de certeza, que un incidente de seguridad ha ocurrido que llevó a que los datos personales se vieran comprometidos ➔ esta confirmación / conocimiento de la violación de la seguridad de los datos personales, con un grado razonable de certeza, activa el inicio del periodo de notificación (72 horas a partir de que se conozca el incidente, para notificar a la ANTAI y a los titulares afectados).

3.3 Una vez que la violación haya sido identificada y confirmada, evaluar el nivel de riesgo que ésta puede suponer

Responsables: Departamento de TI, el Departamento en cuestión, todos los empleados

- **El Departamento de TI y los equipos afectados por el incumplimiento y de los participantes implicados en la gestión de este tipo de eventos**, deberán determinar rápidamente si la violación a la seguridad de los datos personales es probable que resulte en un riesgo para los derechos y libertades de los titulares de datos personales e identificar si este riesgo es alto para poder, como requerido, notificar a la ANTAI y a los titulares afectados dentro del plazos indicado. De lo que se trata es de evaluar la probabilidad de que ocurra y la severidad de las consecuencias de dicha violación. A este respecto, la **ANTAI**, por sí o a través de la Dirección Nacional de Ciberseguridad de la Autoridad Nacional para la Innovación Gubernamental (AIG), difundirá información sobre higiene cibernética, específicamente sobre los Controles de Seguridad en Internet (CIS), un estándar aceptado a nivel mundial; según sea necesario, también podrá proporcionar capacitación a los miembros del sector privado. La Dirección Nacional de Ciberseguridad de la AIG también dirigirá la divulgación para difundir y fomentar el uso de normas y directrices básicas para la ciberseguridad. A través de la Dirección Nacional de Ciberseguridad de la AIG, las entidades del sector privado podrán comunicarse con otras entidades del sector privado sobre la inteligencia cibernética y el intercambio de información sobre amenazas.

- Con ese objetivo, es necesario **tomar en cuenta las circunstancias específicas de la violación**, y en particular:
  - el tipo de violación (confidencialidad, disponibilidad, integridad);
  - la naturaleza, volumen y sensibilidad de los datos (por ejemplo: datos de la tarjeta de crédito o de pago, datos de salud);
  - el número y tipo de los individuos afectados (por ejemplo: individuo vulnerable, menor de edad, paciente);
  - la facilidad para identificar a los individuos;
  - las características del custodio, cuando exista; y
  - la severidad de las consecuencias (riesgos que probablemente resulten en daños físicos, materiales o no materiales como discriminación, robo de identidad, pérdida financiera, daños reputacionales o pérdida de confidencialidad de los datos protegidos por el secreto profesional).

- **A manera de ejemplo**, un ataque a la seguridad de los datos personales en un mercado en línea (acceso, contraseña, historial de compras) es probable que resulte en un alto riesgo. En contraste, el robo de una llave USB que contiene un respaldo de datos cifrados no es probable que resulte en un alto riesgo si los datos están cifrados con un algoritmo de cifrado de última generación, si un respaldo de los datos existe y la clave criptográfica no ha sido comprometida.

3.4 Implementar un plan de acción correctivo

- **En caso de una violación importante** el área de Soporte Técnico e Infraestructura alertará al Director de TI sin dilaciones indebidas de la existencia y del contexto de la violación de la seguridad de los datos personales y de las medidas a ser inmediatamente implementadas.

- **En caso de una violación masiva de datos**, se debe convocar un Comité de respuesta a crisis. El Comité de respuesta a crisis convocará a todos los actores que deban ser involucrados en la gestión de este tipo de eventos: Departamento de TI, Departamento Legal, Departamento de RRHH, el Director del Departamento en cuestión, y el representante de cada filial (unidad de negocio) en cuestión.

- **Si la violación únicamente involucra un incidente de seguridad de TI**, el Comité de respuesta a crisis debe ser convocado en las condiciones previstas en el procedimiento del “Comité de Seguridad TI”.

- **Si no se confirma algún incidente de seguridad de TI** en conexión con la violación, se convocará otra reunión del Comité de respuesta a crisis, en las condiciones previstas en el procedimiento para incidentes no relacionados con TI.

- **Si la violación involucra un incidente de naturaleza mixta** (seguridad de TI, otro), el Comité de respuesta a crisis se reunirá en las condiciones señaladas en los dos párrafos anteriores.

- El **Comité de respuesta a crisis** es responsable en particular de investigar las causas de la violación. Decidirá las medidas físicas y lógicas a ser tomadas para contener la violación y mitigar cualquier efecto adverso posible. También documentará todos los pasos del procedimiento implementado para fines internos de JCDecaux. El Comité de respuesta a crisis también será responsable de cerrar el incidente y establecer un plan de acción para evaluar la calidad de las medidas implementadas y considerar acciones correctivas a ser tomadas para evitar una repetición del incidente.

3.5 Notificar la violación a la autoridad de control (la Autoridad Nacional de Transparencia y Acceso a la Información - ANTAI) y a los titulares afectados

Responsables: Departmento de TI, Departamento Legal

- La ANTAI y los titulares afectados deberán ser notificados únicamente cuando la violación a la seguridad de los datos personales haya sido válidamente establecida.

- **Los titulares de datos personales afectados por una violación de datos personales deben ser informados** dentro del plazo de 72 horas siguientes a la violación (y una vez que dicha violación haya sido identificada y confirmada), para permitir a los titulares que tomen las acciones necesarias para protegerse de potenciales efectos adversos.

- Los titulares de datos personales deberán ser informados **por cualquier medio** que permita una comunicación individual con cada uno de ellos (e-mail, correo, etc.).

- La información debe ser proporcionada a través de **un mensaje dedicado** y no deberá ser enviada con otra información (factura, publicidad de servicios, etc.).

- La notificación estará redactada en un lenguaje claro y sencillo. Se realizará en el plazo de 72 horas a partir de que se conozca el incidente y contendrá, al menos, la siguiente información:
  - La naturaleza del incidente;
  - Los datos personales comprometidos;
  - Las acciones correctivas realizadas de forma inmediata;
  - Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses;
  - Los medios disponibles al titular para obtener mayor información al respecto.

3.6 Documentar toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento

Responsables: el Departamento en cuestión, Departamento de TI, Departamento Legal

- JCDecaux documentará toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, como mínimo, la siguiente información y conservándola a disposición de la ANTAI:
  - La fecha en que ocurrió;
  - El motivo de la violación:
  - Los hechos relacionados con ella y sus efectos;
  - Las medidas correctivas implementadas de forma inmediata y definitiva.