PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

THE TRUST FOR THE AMERICAS

GENERALIDADES DE LA PROTECCIÓN DE DATOS PERSONALES EN COSTA RICA

Julio 2019

CONTENIDOS

- ¿Qué es un dato personal?
  - Tipos de datos
- ¿Qué es el tratamiento de los datos personales?
- Antecedentes en Costa Rica sobre la protección de los datos personales.
- Marco legal sobre la protección de datos personales.
  - Derechos y deberes de los individuos con respecto a los datos personales.
- Principios de la protección de datos personales.
- ¿Qué es la transferencia de datos?
  - Condiciones para la transferencia.
- Excepciones de autodeterminación.
- Pasos a seguir para realizar una denuncia ante la Agencia de Protección de Datos de los Habitantes.
  - Detonantes para un procedimiento de protección de datos.
  - Código penal en referencia a la protección de datos personales.
- Bases de datos que deben inscribirse ante la Agencia de Protección de Datos de los Habitantes.
- Pasos para ejecutar la inscripción.
- Consejos para el adecuado manejo de los datos personales.
- Seguridad de los datos.
  - Medidas de seguridad en el tratamiento de los datos personales.
  - Factores para determinar las medidas de seguridad.
  - Acciones para la seguridad de los datos personales.
  - Actualización de las medidas de seguridad.
  - Protocolos de actuación.
  - Información mínima.
  - Vulnerabilidad de la seguridad.
- Referencias.

INTRODUCCIÓN

El presente manual fue realizado en el mes de julio del 2019, incorporando lo establecido en la Ley N°8968 “Protección de la Persona frente al Tratamiento de sus Datos Personales” y su Reglamento.

La anterior Ley será de aplicación a los datos personales que se encuentren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

Este documento se ha elaborado con le propósito de brindar una guía sobre cómo ejercer la protección de datos personales de los habitantes, y asimismo, exponer algunas generalidades sobre la normativa.

¿Qué es un dato personal?

Corresponde a cualquier dato relativo a una persona física identificada o identificable.

Tipos de datos

- Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
- Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.
- Datos sensibles: es toda información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

¿Qué es el tratamiento de los datos personales?

Es cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

Antecedentes en Costa Rica sobre la protección de los datos personales.

Previo a la creación de la Ley 8968, Costa Rica contaba con el siguiente marco normativo:

- Art. 24 Constitución Política. Derecho intimidad, libertad y secreto de comunicaciones.
- Art. 47 Código Civil. Derecho a la imagen.
- Art.615 Código de Comercio. Secreto bancario.
- Art. 27 y 41 Ley Orgánica Organismo de Investigación Judicial (OIJ). Carácter confidencial e interno del OIJ a nivel de investigaciones.
- Leyes sectoriales.
- Sala Constitucional. Habeas Data.

Marco legal sobre la protección de datos personales.

Costa Rica posee la Ley N° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, la cual fue publicada en el Diario Oficial la Gaceta el 5 de setiembre del 2011.

Nació con el objetivo de garantizar a cualquier persona el respeto a sus derechos fundamentales y derechos de la personalidad, concretamente, su derecho a la Autodeterminación Informativa y la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos, correspondientes a su persona o bienes.

Derechos y deberes de los individuos con respecto a los datos personales

Los habitantes gozarán de los siguientes derechos con respecto a la protección de sus datos personales:

● Acceso a la información: la información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada.

● Derecho de rectificación: Se garantiza el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente Ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.

Por otro lado, los responsables de las bases de datos tienen obligaciones ante la Ley. En primer lugar, la persona responsable de la base de datos debe resolver lo solicitado por el titular de los datos (derecho de acceso y/o rectificación), de manera gratuita, en el plazo de cinco días hábiles contados a partir de la recepción de la solicitud.

Principios de la protección de datos personales

● Principio de consentimiento informado:

○ Obligación de informar: cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco.

○ Otorgamiento de consentimiento: quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Además, deberá constar por escrito, ya sea en un documento físico o electrónico, y podrá ser revocado cuando el titular así lo solicite.

○ Este consentimiento deberá ser libre, específico, informado e inequívoco.

● Principio de calidad de la información: sólo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos cumplan con ser actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.

¿Cuáles son las características de una información de calidad?

● Actualidad: los datos de carácter personal deberán ser actuales, por lo tanto, el responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular.

● Veracidad: Los datos de carácter personal deberán ser veraces. La persona responsable de la base de datos está obligada a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita.

● Exactitud: los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a

los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Adicionalmente, si los datos de carácter personal registrados son inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección.

● Adecuación al fin: los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente para otros fines fuera de lo establecido.

¿Qué es la transferencia de datos?

Acción mediante la cual se trasladan datos personales del responsable de una base de datos personales a cualquier tercero distinto del propio responsable, de su grupo de interés económico, del encargado, proveedor de servicios o intermediario tecnológico, en estos casos siempre y cuando el receptor no use los datos para distribución, difusión o comercialización.

Condiciones para la transferencia.

Para llevar a cabo una transferencia de información personal debe cumplirse lo siguiente:

● Requiere el consentimiento inequívoco del titular, salvo disposición legal en contrario.

● Los datos a transferir deben haber sido recabados o recolectados de forma lícita.

● No se considera transferencia el traslado de datos personales del responsable de una base de datos a un encargado, proveedor de servicios o intermediario tecnológico o las empresas del mismo grupo de interés económico.

● El responsable de la transferencia de datos personales deberá establecer un contrato con el responsable receptor, en el que se prevean, al menos las mismas obligaciones a las que se encuentra sujeto el responsable de la transferencia de dichos datos.

Excepciones de la Autodeterminación Informativa

Se presentará una limitación de los principios, derechos y garantías de forma justa, razonable y según el principio de transparencia administrativa, cuando se persigan los siguientes fines:

● La seguridad del Estado.

● La seguridad y el ejercicio de la autoridad pública.

● La prevención, persecución, investigación, detención y represión de las infracciones penales o de las infracciones de la deontología en las profesiones.

● El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.

● La adecuada prestación de servicios públicos.

● La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

Pasos a seguir para realizar una denuncia ante la PRODHAB

Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar ante la PRODHAB que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la Autodeterminación Informativa establecidas en esta Ley.

- Imprimir el formulario denominado “Procedimiento de Protección de Datos”.
- Completar el formulario, firmar el documento y adjuntar las evidencias.
- Presentarlo ante la Agencia de Protección de Datos Personales de los Habitantes.

Detonantes para un procedimiento de protección de derechos

Los detonantes para el desarrollo del debido procedimiento de protección de datos personales son los siguientes:

- Se recolecten, almacenen, transmitan, transfieran o se empleen datos personales en contravención de las reglas establecidas en la Ley y el Reglamento de la misma.
- Se niegue, de forma injustificada, a dar acceso, eliminar o rectificar a un titular sobre los datos que consten en archivos y bases de datos.
- Se transfieran, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares.
- Se realice tratamiento de datos personales sin encontrarse debidamente inscrito ante la Agencia.

Código Penal en referencia a la protección de datos personales

De acuerdo con la normativa establecida y específicamente con el Artículo 196 bis. - Violación de datos personales, se define:

Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

- Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
- La información vulnerada corresponde a un menor de edad o incapaz.
- Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona. (…)

Por otro lado, con respecto a la captación indebida de manifestaciones verbales, se encuentra especificado en el Artículo 198, el cual establece lo siguiente.

Será reprimido, con prisión de uno a tres años, quien grabe sin su consentimiento, las palabras de otro u otros, no destinadas al público o que, mediante procedimientos técnicos, escuche manifestaciones privadas que no le estén dirigidas, excepto lo previsto en la Ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones. La misma pena se impondrá a quien instale aparatos, instrumentos, o sus partes, con el fin de interceptar o impedir las comunicaciones orales o escritas, logren o no su propósito.

Continuando con lo anterior, el Artículo 200. define, en los casos de los tres artículos anteriores, se impondrá prisión de dos a seis años si la acción se perpetra:

- Por funcionarios públicos, en relación con el ejercicio de sus funciones.
- Por quien ejecute el hecho, prevaliéndose de su vinculación con una empresa o institución pública o privada encargada de las comunicaciones.
- Cuando el autor publique la información obtenida o aún sin hacerlo, tenga carácter privado, todo a juicio del Juez.

Bases de datos que deben inscribirse ante la PRODHAB

De acuerdo con la Ley N°8968, toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que habilite PRODHAB.

La inscripción no implica la transferencia de los datos a la Agencia de Protección de Datos.

Pasos para ejecutar la inscripción

A fin de llevar a cabo la debida inscripción de una base de datos ante la Agencia de Protección de Datos son los siguientes:

- Presentar el formulario de inscripción del registro de la base de datos personales ante la Agencia y aportar los requisitos adicionales.
- Si la solicitud de inscripción no cumple con los requisitos exigidos, la Agencia requerirá que el solicitante subsane la omisión. De no hacerlo, se procederá al archivo.
- Cumplidos los requisitos o subsanada la prevención, el solicitante debe cancelar el canon de Regulación y Administración, así como el de comercialización si corresponde. De no realizarlo en el plazo establecido, se archivará la gestión.
- La Dirección de la Agencia, dictará una vez sea recibido el pago del canon, la resolución de inscripción del registro de la base de datos.
- Contra la resolución final al procedimiento de inscripción del registro de la base de datos, procederá la interposición de los recursos ordinarios de Reconsideración y Apelación.

Consejos para el adecuado manejo de los datos personales

Se recomienda a los usuarios tomar en cuenta los siguientes consejos brindados por la Agencia de Protección de Datos:

- Cuando se le solicite sus datos personales, consultar sobre la finalidad, alcances y si será compartida, cedida o vendida a terceros.
- Maximizar el nivel de privacidad de sus redes sociales y prestar atención a lo que publica.
- Concientizar a sus hijos sobre la importancia de la protección de los datos personales.
- En el caso de los datos sensibles debe mediar siempre el consentimiento informado.

Seguridad de los datos

El responsable del manejo de las base de datos deberá de adoptar las medidas de índole técnica y de organización necesarias a fin de garantizar la seguridad de los datos de carácter personal y evitar la alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado de los mismos.

Estas medidas deben incluir mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

Asimismo, no se registra aquellos datos personales en base de datos que no posean las condiciones que garanticen la seguridad e integridad, ni los equipos, centros de tratamiento, sistemas o programas.

Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Medidas de seguridad en el tratamiento de los datos personales

Se entenderá por medidas de seguridad el control o grupo de controles para proteger los datos personales.

Factores para determinar las medidas de seguridad

El responsable determinará las medidas de seguridad, aplicables a los datos personales que trate o almacene, considerando los siguientes factores:

- La sensibilidad de los datos personales tratados, en los casos que la ley lo permita.
- El desarrollo tecnológico.
- Las posibles consecuencias de una vulneración para los titulares de sus datos personales.
- El número de titulares de datos personales.
- Las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento.
- El riesgo por el valor, cuantitativo o cualitativo, que pudieran tener los datos personales.
- Demás factores que resulten de otras leyes o regulación aplicable al responsable.

Acciones para la seguridad de los datos personales

A fin de establecer y mantener la seguridad física y lógica de los datos personales, el responsable deberá realizar al menos las siguientes acciones, las cuales podrán ser requeridas en cualquier momento por la Agencia:

- Elaborar una descripción detallada del tipo de datos personales tratados o almacenados.
- Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias.
- Señalar el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos; igualmente, indicarse el nombre y la versión de la base de datos utilizada cuando proceda.
- Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales.
- Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva;
- Calcular el riesgo residual existente basado en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo residual.

Actualización de las medidas de seguridad

Se lleva a cabo las respectivas modificaciones a las medidas o procesos de seguridad para su mejora continua, asimismo, se produzcan modificaciones sustanciales en el tratamiento o almacenamiento o, que deriven un cambio del nivel de riesgo.

Dichas actualizaciones se originarán al ser vulnerables los sistemas de tratamiento o almacenamiento o de datos personales o el presentarse una afectación a los datos personales, distinta a las anteriores.

Protocolos de actuación

Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta Ley.

Continuando con lo anterior, a fin de que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Agencia de Protección de Datos, la cual podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.

La manipulación de datos con base en un protocolo de actuación inscrito ante la hará presumir, "iuris tantum", lo cual implica el cumplimiento de lo establecido en la Ley N° 8968, para los efectos de autorizar la cesión de los datos contenidos en una base.

Información mínima

El responsable deberá informar al titular y a la Agencia, en caso de vulnerabilidades de seguridad, al menos lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios o el lugar, donde puede obtener más información al respecto.

Vulnerabilidad de la seguridad

El responsable deberá informar al titular sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá cinco días hábiles a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

Dentro de este mismo plazo deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan.

Referencias

http://www.prodhab.go.cr//reformas/