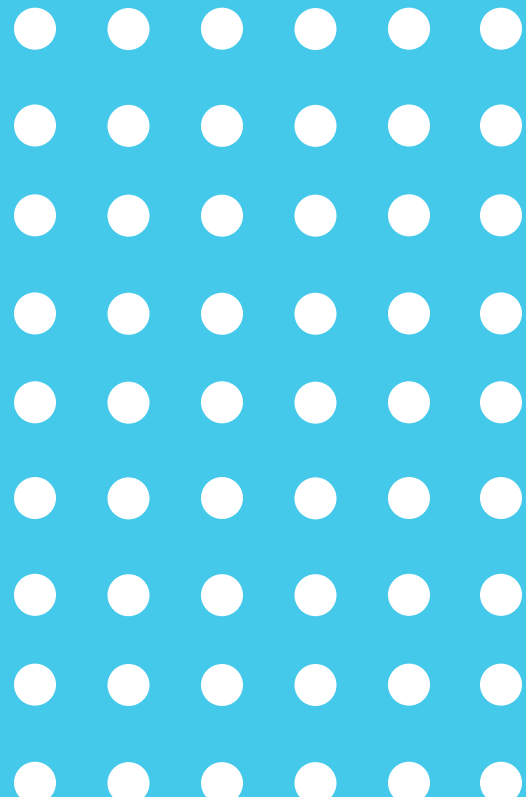
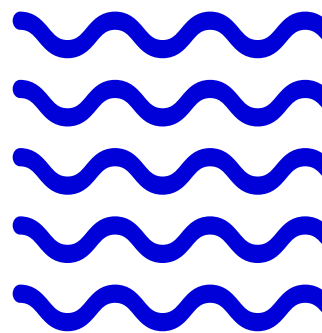


Estudio Centroamericano de Protección de Datos,

GUATEMALA

Sara Fratti





Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0):
<https://creativecommons.org/licenses/by-sa/4.0/>

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Coordinación: Lia Hernández
Autoría: Sara Fratti

Enero 2019.



Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

1. Marco jurídico constitucional

En su Artículo 24, la Constitución Política de la República de Guatemala¹ establece la inviolabilidad de la correspondencia como un derecho fundamental, el cual regula de la siguiente manera:

“La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley.

Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio”.

En consecuencia, la norma constitucional establece como garantía la protección e inviolabilidad de los documentos (y su contenido). Es importante mencionar que en el referido artículo se enumeran las comunicaciones que son protegidas, sin ser ésta restrictiva, pues contempla en cierta medida los avances de la tecnología moderna.

El Artículo 31 de la Constitución se regula la autodeterminación informativa como un derecho que puede ser ejercida por las y los ciudadanos ante las entidades públicas que posean registros con información personal. El cual determina que “toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos”.

¹ Asamblea Nacional Constituyente. Constitución Política de la República de Guatemala. Disponible en: https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf

2. Marco jurídico ordinario

Guatemala carece de una normativa de protección de datos. Sin embargo, en el año 2009 se presentó en el Congreso de la República la Iniciativa 4090² que dispone aprobar la Ley de Protección de Datos Personales, la cual ya posee dictamen favorable emitido por la Comisión de Economía y Comercio Exterior pero que desde el año 2010 se encuentra pendiente del tercer debate y aprobación final por el Pleno del Congreso.

El Decreto Número 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública³, fue emitido el 23 de septiembre del 2008 y entró en vigencia el 20 de abril del 2009.

Es importante destacar que a pesar que no existe una legislación específica sobre protección de datos personales, la Ley de Libre Acceso a la Información Pública actualmente es la única que regula lo referente a los datos personales y datos sensibles, así como establece un mecanismo de protección de estos y tipifica delitos en la materia.

² Congreso de la República de Guatemala. Iniciativa 4090, Ley de Protección de Datos Personales. Disponible en: <https://www.congreso.gob.gt/wp-content/plugins/paso-estado-incidencias/includes/uploads/docs/988.pdf>

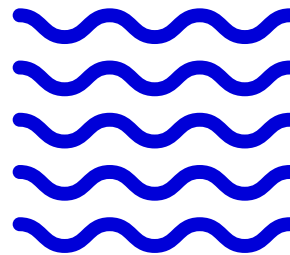
³ Congreso de la República de Guatemala. Decreto Número 57-2008, Ley de Acceso a la Información Pública. Disponible en: https://www.oas.org/juridico/pdfs/mesicic4_gtm_acceso.pdf

3. Definición de datos personales

La Ley de Libre Acceso a la Información Pública en el Artículo 9 determina y define los datos personales y los datos personales sensibles. Siendo los primeros “los relativos a cualquier información concerniente a personas naturales identificadas o identificables”.

En tanto, los datos personales sensibles se refieren a “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar y otras cuestiones íntimas de similar naturaleza”. Asimismo, en el Artículo 22 numeral 5, se determina que los datos sensibles son confidenciales.

Por su parte, la Iniciativa 4090 define en el Artículo 3 que los datos de carácter personal “es cualquier información relativa a una persona individual identificada o identificable”; además, define los datos sensibles como “aquellos datos personales que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida sexual y antecedentes delictivos, operaciones bancarias, registros tributarios, aduaneros o relativos a actividades económicas”.



4. Principios de tratamiento de datos personales

Existen principios fundamentales para la protección de los datos personales que sirven de fundamento al derecho de intimidad de las personas, en torno al tratamiento que reciben por parte de la Administración Pública y empresas. En este sentido, la Iniciativa de Ley de Protección de Datos Personales determina como principios básicos los siguientes:

A. Calidad de los datos:

En el artículo 6 se determina que el procedimiento y tratamiento de los datos personales deben ser adecuados, pertinentes y no excesivos al fin legítimo para el cual se recopilaron. Además, determina cuándo se deben cancelar los datos, como en caso que no exista consentimiento legal, sean inexactos e incompletos, ya no sean pertinentes o necesarios.

Por su parte, el inciso h) establece que es obligatoria la cancelación de los datos personales en caso de fallecimiento del titular, para lo cual las instituciones tendrán plazo de un año para realizar la cancelación.

B. Transparencia:

El artículo 4 de la referida iniciativa indica que las personas, individuales o jurídicas, que solicitan datos personales deberán informar de manera previa, expresa, precisa e inequívoca lo siguiente: la existencia del archivo, manual o automatizado, la finalidad y destinatarios. De la misma manera, deben informarle a la persona los derechos que posee.

C. Conservación:

La iniciativa 4090 en su Artículo 6, inciso f) que los datos personales serán conservados únicamente en la manera que no permita la identificación de su titular y por un período razonable y necesario para el cual fueron registrados. Además, determina que “en ningún caso, serán conservados los datos personales que puedan afectar de cualquier modo a su titular, una vez transcurridos diez (10) años desde la fecha de ocurrencia de los hechos registrados, salvo disposición legal en contrario”.

D. Seguridad de los datos:

Conforme los Artículos 8 y 9 de la iniciativa, los responsables de los archivos, ficheros, registros o bases de datos, públicos o privados, deberán adoptar las medidas necesarias para garantizar la seguridad de los datos personales con el fin de evitar su alteración, pérdida o acceso no autorizado.

En este sentido, la legislación también impondría la obligación de confidencialidad a las personas responsables del tratamiento de los datos personales, aún después de finalizar su relación con el archivo de datos.



5. Derechos ARCO

Los titulares de los datos personales tienen los derechos de acceso, rectificación, cancelación y oposición, los cuales son conocidos como los derechos ARCO. En el Artículo 13 de la Iniciativa de Protección de Datos Personales se regulan como parte del derecho de acceso a la información.

Por un lado, el titular posee el derecho de acceder a la información y datos personales que está en un archivo, lo cual le permite conocer qué clase de datos posee alguna institución o empresa, así como conocer la finalidad para la cual fueron recopilados. Este derecho permite al titular de los datos personales actualizarlos o rectificarlos en caso que sean inexactos o incompletos, lo cual le permite al titular tener control sobre la información que se manejan en los registros. Además, también posee los derechos de oposición y cancelación, en caso que crea necesario que los datos personales ya no consten en los registros o archivos, los casos en los que procede la cancelación ya se indicaron anteriormente.

6. Consentimiento

El Artículo 5 de la Iniciativa 4090 establece los alcances del consentimiento del titular. Es la regla general para la entrega de datos personales, la cual se debe realizar por escrito y de manera física o digital. Además, puede ser revocado. La iniciativa establece las excepciones al consentimiento, como la orden de juez competente y cuando los datos personales se obtienen a través de fuentes de acceso público.

7. Sujetos obligados

Actualmente, de conformidad con el Artículo 6 de la Ley de Acceso a la Información Pública, comprende a los sujetos obligados que sean “persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución o entidad del Estado, organismo, órgano, entidad, dependencia, institución y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del Estado, o actos de la administración pública en general...”.

A pesar que se refiera a estos como obligados a proporcionar la información pública que se les solicite, el Artículo 30 les impone algunas responsabilidades y obligaciones frente al tratamiento de los datos personales, el cual se analizará con detalle más adelante.

Por otro lado, en el Artículo 2 de la Iniciativa de Ley de Protección de Datos Personales se establecen como sujetos obligados a los Organismos del Estado, organizaciones no gubernamentales, lucrativas o no lucrativas y empresas que posean un archivo, manual o automatizado, de datos personales, con excepción de los archivos regulados por la Ley Electoral y de Partidos Políticos y los que deriven del Registro Civil y del Registro Nacional de las Personas.

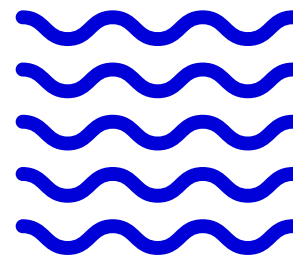
8. Obligaciones y responsabilidades de los sujetos obligados

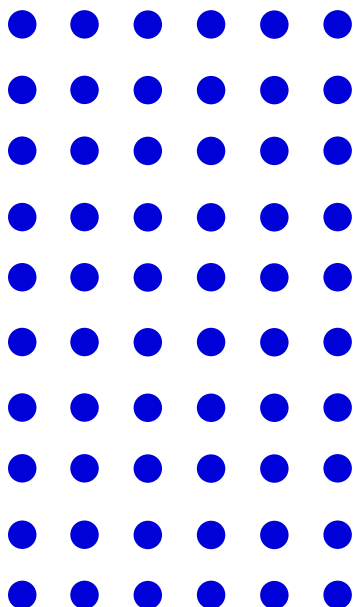
Conforme al Artículo 30 de la Ley de Acceso a la Información Públicas, los sujetos poseen las siguientes obligaciones:

- 1.** “Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean, presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos.
- 2.** Administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido.
- 3.** Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento.
- 4.** Procurar que los datos personales sean exactos y actualizados.
- 5.** Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Los sujetos activos no podrán usar la información obtenida para fines comerciales, salvo autorización expresa del titular de la información”.

La iniciativa de Protección de Datos Personales, por su parte, establece varias obligaciones a las personas, individuales o jurídicas, que tienen a su cargo el tratamiento de datos personales, como por ejemplo la adopción de medidas de seguridad de los registros y archivos, confidencialidad, calidad de los datos, entre otras.





9. Transferencia y cesión de datos

El Artículo 10 de la Iniciativa 4090 determina las condiciones relacionadas a la cesión a terceros de los datos personales, los cuales únicamente pueden ser cedidos con el consentimiento previo de su titular. De la misma manera, se establecen las excepciones a éste cuando es exigido por ley, por razones de investigación científica, utilidad pública, seguridad pública y datos sobre estadísticas y censos poblacionales.

10. Autoridad Competente

Actualmente, la autoridad reguladora que determina la Ley de Acceso a la Información Pública es el Procurador de los Derechos Humanos, quien es la autoridad que se encarga de proteger el derecho de acceso a la información pública.

Por su parte, en el marco de la Iniciativa 4090 se establecería la Dirección para la Protección de Datos Personales como un órgano desconcentrado de la oficina del Procurador de los Derechos Humanos, la cual estaría a cargo de un Director nombrado a través de concurso público por el Procurador para un período de 5 años.

11. Procedimientos y Sanciones

La Ley de Acceso a la Información Pública regula el Hábeas Data enfocado como un procedimiento para que los titulares puedan acceder y modificar sus datos personales. Por un lado, el Artículo 33 determina el procedimiento específico para el acceso a la información relacionada a los datos personales que estén en archivos, la cual se le entregará dentro de los 10 días hábiles siguientes a la solicitud. En relación al procedimiento para la modificación de los datos personales, el Artículo 34 establece que se realizaran las modificaciones requeridas con la documentación que motive la solicitud; en un plazo no mayor a 30 días hábiles, el sujeto obligado deberá emitir resolución en la que conste la modificación correspondiente.

El artículo anterior establece un marco general relacionado a las sanciones administrativas, sin embargo, no ahonda en más detalles. Por otro lado, si tipifica un catálogo de delitos en la materia, que requieren la presentación de una denuncia ante un Juzgado de Primera Instancia Penal. Los delitos son:

- **Comercialización de datos personales.**
Consiste en la comercialización o distribución de datos personales o datos sensibles sin la autorización del titular. Se sanciona con prisión de 5 a 8 años, multa de Q.50,000.00 a Q.100,000.00 y comiso de los instrumentos del delito. Artículo 64.
- **Alteración o destrucción de información en archivos.**
Se refiere a la alteración o destrucción, sin autorización, de datos personales o datos sensibles. Se sanciona con prisión de 5 a 8 años y multa de Q.50,000.00 a Q.100,000.00. Artículo 65.

En cambio, en la Iniciativa de Ley de Protección de Datos Personales se determina un régimen disciplinario de carácter administrativo en el caso que los responsables de los archivos y de su tratamiento incumplieren con lo contenido en la ley. Es regulado en los Artículos 30 al 38, en los que establece quién puede interponer una denuncia ante la Dirección para la Protección de Datos Personales, además de los plazos respectivos al trámite de la misma.

En relación a las sanciones contenidas en la Iniciativa 4090, en el Artículo 35 se establece el catálogo de sanciones administrativas que impondría la Dirección y que consisten en imposición de multa, suspensión parcial y definitiva del funcionamiento del archivo.

12. La computación en la nube y los servicios financieros

La Ley de Bancos y Grupos Financieros⁴, Decreto Número 19-2002, tiene por objeto regular todas las actividades relacionadas a los bancos y grupos financieros que operan en el país, así como a las entidades fuera de plaza (offshore).

Sin embargo, frente a una economía digital competitiva, carece de la normativa adecuada al entorno digital. No se han presentado reformas a la Ley con la finalidad de actualizarla a temas actuales, como la computación en la nube, criptomonedas o FinTech.

13. Agenda Digital

En el año 2016 se presentó la agenda digital del país, denominada Nación Digital 2016-2032, la cual fue elaborada por la Superintendencia de Telecomunicaciones (SIT) con el apoyo de otras entidades gubernamentales.

La agenda digital posee los ejes de acción para el desarrollo de políticas públicas enfocadas en la utilización de las Tecnologías de la Información y Comunicación en las áreas de salud, educación, seguridad, desarrollo y transparencia. Sin embargo, Nación Digital⁵ no recoge estándares internacionales enfocados a la protección de los datos personales y privacidad de la población guatemalteca.

⁴ Congreso de la República de Guatemala. Decreto Número 19-2002, Ley de Bancos y Grupos Financieros. Disponible en: https://www.banguat.gob.gt/leyes/2013/ley_bancos_y_grupos_financieros.pdf

⁵ Nación Digital. <https://1e8q3q16vyc81g8i3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/1.-Agenda-Nacio%CC%81n-Digital-2017.pdf>

Referencias

Asamblea Nacional Constituyente.

Constitución Política de la República de Guatemala. Disponible en: https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf

Congreso de la República de Guatemala.

Iniciativa 4090, Ley de Protección de Datos Personales. Disponible en: <https://www.congreso.gob.gt/wp-content/plugins/paso-estado-incidencias/includes/uploads/docs/988.pdf>

Congreso de la República de Guatemala.

Decreto Número 57-2008, Ley de Acceso a la Información Pública. Disponible en: https://www.oas.org/juridico/pdfs/mesicic4_gtm_acceso.pdf

Congreso de la República de Guatemala.

Decreto Número 19-2002, Ley de Bancos y Grupos Financieros. Disponible en: https://www.banguat.gob.gt/leyes/2013/ley_bancos_y_grupos_financieros.pdf

Nación Digital.

<https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/1.-Agenda-Nacio%CC%81n-Digital-2017.pdf>

