Versión revisada y modificada a julio 2024

Artículo 1. Objeto de La Ley

La presente ley tiene por objeto la protección integral de los datos personales de las personas físicas a fin de garantizar el ejercicio pleno de sus derechos, y el libre flujo de la información, de conformidad a lo establecido en la Constitución Nacional, los tratados internacionales, acuerdos y convenios de los cuales la República del Paraguay es parte.

Artículo 2. Ámbito de Aplicación

La presente ley aplica a cualquier tratamiento de datos personales, total o parcialmente automatizado así como al tratamiento no automatizado, por personas físicas o jurídicas, independientemente del medio, país de su sede o el país donde se encuentren los datos, efectuado:

1. Por un responsable o encargado establecido en territorio nacional, aun si el tratamiento de datos tuviese lugar fuera de dicho territorio;
2. Por un responsable o encargado no establecido en territorio nacional, en los siguientes casos:

    a. cuando realice tratamiento de datos de personas físicas situadas en territorio paraguayo, salvo en casos de fines de tránsito;

    b. cuando las actividades del tratamiento de datos estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de la República del Paraguay;

    c. cuando las actividades de tratamiento de datos estén relacionadas con el control del comportamiento de personas físicas, en la medida en que éste tenga lugar en el territorio de la República del Paraguay.

    d. cuando resulte aplicable la legislación nacional derivada de la celebración de un contrato o en virtud del derecho internacional público.

El tratamiento no automatizado estará sujeto a lo dispuesto en la ley, cuando se trate de datos personales que forman parte de un archivo, o estén destinados a serlo.

Artículo 3. Excepciones a la ley

Se considera exento de aplicación de la presente ley, el tratamiento de datos cuando los datos personales estén destinados a actividades exclusivamente en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.

La aplicación de la presente Ley no podrá afectar el secreto de las fuentes de información periodística.

La presente ley no se aplica al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención de amenazas para la seguridad pública.

Artículo 4. Limitaciones al derecho de la protección de datos

Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Constitución Nacional y reglamentados por la presente ley, deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto de los principios de razonabilidad y minimización, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por el Estado o a la necesidad de protección de los derechos y libertades de los demás.

Artículo 5. Definiciones

A los efectos de la presente ley, se consideran las siguientes definiciones:

1. **Anonimización:** La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona física.
2. **Bloqueo de datos:** La identificación y reserva de datos personales, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, fiscalía y demás autoridades públicas competentes, en la forma y condiciones establecidas en las normas vigentes.
3. **Consentimiento:** Toda manifestación de voluntad libre, previa,expresa, específica, informada e inequívoca por la que una persona física acepta y autoriza, ya sea mediante una declaración o una clara acción afirmativa realizada por escrito o por medios electrónicos, así como por cualquier forma equivalente que la tecnología permita, el tratamiento de los datos personales que le conciernen.
4. **Datos Biométricos:** Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, tales como imágenes faciales o datos dactiloscópicos.
5. **Datos Genéticos:** Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
6. **Datos Personales:** Información de cualquier tipo referida a personas físicas determinadas o determinables. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Los datos personales de las personas físicas constituyen información de carácter reservado.
7. **Datos Personales Sensibles:** Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa y no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical opolítica; datos relativos a la salud, a la preferencia u

orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

8. **Elaboración de Perfiles:** Toda forma de tratamiento automatizado y parcialmente automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos de una persona física, en particular para analizar o predecir cuestiones relativas al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etnia, raza, sexo o movimientos de dicha persona física.
9. **Encargado Del Tratamiento:** La persona física o jurídica, autoridad pública, u otro organismo que trate datos personales en representación o mandato del responsable del tratamiento
10. **Evaluación de Impacto Relativa A La Protección De Datos:** Análisis de carácter previo de acuerdo a las disposiciones de la ley y para los casos que ésta disponga, para aquellos tratamientos de datos que puedan suponer un riesgo para los derechos y libertades de las personas.
11. **Incidente de seguridad de datos personales:** Toda violación que ocasiona la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratado de otra forma, o la comunicación o acceso no autorizados a dichos datos.
12. **Mecanismos de autorregulación vinculante:** Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento para transferencias de datos personales conforme a los principios legalmente establecidos, a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o asociaciones u organismos representativos de categorías de responsables o encargados.
13. **Representante:** La persona física o jurídica establecida en la República del Paraguay que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente a aquel en lo que respecta a sus respectivas obligaciones en virtud de la presente ley.
14. **Responsable del Tratamiento:** La persona física o jurídica, autoridad pública u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de los datos personales, sujeto a los deberes y obligaciones que la ley establece.
15. **Seudonimización:** El tratamiento de datos personales de manera tal que ya no pueda atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional se conserve por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar la protección de la identidad del titular.
16. **Tercero:** La persona física o jurídica, nacional o extranjera, pública o privada, distinta del titular de los datos, del responsable, del encargado y de las personas que, bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento, estén autorizadas a tratar datos personales.
17. **Titular de Datos:** Persona física sobre la cual se realiza el tratamiento de sus datos personales.
18. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales, automatizados o parcialmente automatizados, realizadas sobre datos personales, relacionadas de manera enunciativa más no limitativa, con la obtención, acceso, recolección, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, bloqueo, elaboración, transferencia, cesión, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Artículo 6. Principio de exactitud de los datos

Los datos personales serán veraces, exactos, completos y actualizados. Los responsables y encargados del tratamiento deben adoptar todas las medidas razonables para corregir errores, modificar los datos que resulten ser falsos, inexactos, desactualizados o incompletos y garantizar la certeza y veracidad de la información objeto de tratamiento.

En los casos en que los datos son proporcionados por su titular, se presume su exactitud.

Artículo 7. Principio de licitud del tratamiento

Para que el tratamiento sea lícito, los datos personales deben ser tratados conforme a las bases jurídicas previstas en la presente ley en el artículo 24, así como el conjunto de principios y demás disposiciones de la ley y sus reglamentaciones

Artículo 8. Principio de finalidad

Los datos personales deben ser recogidos y procesados con fines determinados, explícitos, legítimos y de duración limitada, y no serán tratados, posteriormente, de manera incompatible o distinta con dichos fines.

El tratamiento ulterior de los datos personales con fines de archivo e interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales, siempre que se encuentren anonimizados o se respete la protección establecida en la ley.

Artículo 9. Principio de minimización

El responsable y el encargado tratarán únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.
Asimismo, los datos deberán someterse a revisión periódica para determinar si continúan cumpliendo la finalidad.

Artículo 10. Principio de lealtad

No podrán recabarse datos personales por medios o métodos fraudulentos, engañosos, desleales o ilícitos, lo que implica que:

a. No se recaben datos personales con dolo, mala fe o negligencia.
b. No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado.
c. Se informen todas las finalidades del tratamiento.

Artículo 11. Principio de transparencia

El responsable informará al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Esta información será fácilmente accesible, en lenguaje claro y sencillo.

Artículo 12. Principio de conservación de datos personales

No podrán conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento. El Responsable del tratamiento deberá establecer los plazos para la supresión y/o revisión periódica.

Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

Artículo 13. Principio de responsabilidad proactiva

El responsable y encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la Autoridad de Control su efectiva implementación.

Artículo 14. Principio de seguridad

En el tratamiento de datos personales se deberán adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos y que tendrán como finalidad evitar la alteración, pérdida, tratamiento o acceso no autorizado. En el caso de datos definidos por esta ley como datos sensibles, se adoptarán medidas adicionales para garantizar la seguridad de estos ante los riesgos específicos relacionados al tratamiento de dichos datos.

El responsable y el encargado del tratamiento llevarán a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

La Autoridad de Control reglamentará las condiciones técnicas de seguridad e integridad mínimas que deberán ser aplicadas por los responsables y encargados del tratamiento.

Artículo 15. Principio de confidencialidad

Los responsables y encargados del tratamiento de datos de carácter personal, así como toda persona que intervenga en cualquier fase de este estarán sujetas al deber de confidencialidad, obligación que subsistirá aun después de finalizar sus relaciones con el titular. Los mismos podrán ser relevados del deber de confidencialidad por resolución judicial u obligación legal.

Artículo 16. Disposiciones Generales Sobre El Ejercicio De Los Derechos

El titular de datos o su representante podrán, en cualquier momento, solicitar al responsable, el acceso, rectificación, supresión, oposición y portabilidad de los datos personales que le conciernen.

El ejercicio de cualquiera de los derechos mencionados no es requisito previo ni impide el ejercicio de otro.

El responsable deberá establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular de datos ejercer sus derechos.

El responsable tendrá un plazo de 10 (diez) días hábiles computados desde la presentación de la solicitud para dar respuesta a la solicitud del Titular.

Vencido el plazo sin que se satisfaga el pedido, o si para el titular de los datos la respuesta fuera insuficiente, se podrá recurrir ante la Autoridad de Control o, si correspondiere, podrá interponer la acción de habeas data. En caso de optar por la acción de habeas data, o de haberla iniciado con anterioridad, no podrá iniciar el trámite ante la Autoridad de Control.

El ejercicio de los derechos previstos en el presente capítulo es irrenunciable. En el caso de titulares de los datos de personas fallecidas, les corresponde a sus sucesores universales.

Artículo 17. Derecho a la Información

El titular de datos debe recibir la información sobre cómo se lleva a cabo el tratamiento de sus datos personales, ya sea que lo haya proporcionado directamente a un responsable de tratamiento o que el responsable lo haya obtenido de otra fuente.

El responsable proporcionará al titular, al momento de la obtención de los datos, al menos, la información siguiente:

a. Las categorías de datos personales que serán objeto del tratamiento;
b.Su identidad y datos de contacto que son el domicilio legal, número de teléfono y correo electrónico.
b. Base legal y finalidades del tratamiento a que serán sometidos sus datos personales.
c. Las comunicaciones o transferencias internacionales de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de estas.
d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, oposición, supresión y portabilidad.
e. Tiempo de conservación de los datos personales, o en su defecto, el criterio utilizado para determinar el periodo de tiempo.
f. La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 23 y, al menos en tales casos, información significativa sobre la lógica aplicada, sin que ello afecte derechos intelectuales del responsable del tratamiento.
g. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.
h. El derecho a recurrir ante la Autoridad de Control.

La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

La información facilitada, así como la comunicación y cualquier actuación realizada debe ser a título gratuito. Salvo cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costos administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Si el responsable del tratamiento tiene dudas razonables en relación con la identidad de la persona física que realiza la solicitud, podrá requerir información adicional necesaria para confirmar la identidad del interesado.

Artículo 18. Derecho De Acceso

El titular de datos tendrá el derecho a solicitar y obtener sus datos personales que obren en posesión del responsable y/o una copia de los mismos. Previa acreditación de su identidad, la información deberá ser suministrada en forma clara, inteligible y exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje accesible al conocimiento medio de la población.
En ningún caso el informe puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el titular de los datos. La información, a opción del titular de los datos, puede suministrarse por escrito, por medios electrónicos, de imagen u otro idóneo a tal fin.

Artículo 19. Derecho De Rectificación

El titular de datos tendrá el derecho a obtener del responsable la rectificación de sus datos personales, cuando éstos resulten ser inexactos, falsos, erróneos, incompletos o no se encuentren actualizados.

En el supuesto de cesión o transferencia internacional de datos erróneos o desactualizados, el responsable del tratamiento debe notificar la rectificación al cesionario dentro del quinto (5°) día hábil de haber tomado conocimiento efectivo del error o la desactualización.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable del tratamiento debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión.

Artículo 20. Derecho De Oposición

El titular del dato tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de los datos personales que le conciernen, incluida la elaboración de perfiles basados en dichas disposiciones. El responsable del tratamiento dejará de tratar los datos

personales objeto de oposición, a menos que demuestre motivos legítimos para el procesamiento que prevalezcan sobre los intereses, derechos y libertades del titular del dato o para el reconocimiento, ejercicio o defensa de reclamaciones legales.
Cuando el titular de datos se oponga al tratamiento de sus datos personales, estos dejarán de ser tratados en un plazo de 10 (diez) días hábiles desde el envío de la solicitud de oposición.

Cuando el titular de datos se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines en un plazo de 10 (diez) días hábiles desde el envío de la solicitud de oposición.

Artículo 21. Derecho De Supresión

El titular de datos tendrá derecho a solicitar la eliminación de sus datos personales de los archivos, registros, bases de datos y sistemas del responsable, a fin de que los mismos dejen de ser tratados por este último.

Podrá requerirse en los siguientes casos:

1. Los datos personales hayan sido tratados ilícitamente;
2. Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
3. Haya vencido el plazo de conservación de los datos personales;
4. El titular de datos haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna o éste no se ampare en otro fundamento jurídico;
5. El titular de los datos haya ejercido su derecho de oposición conforme al artículo 20, y no prevalezcan otros motivos legítimos para el tratamiento de sus datos;
6. Los datos personales que deban suprimirse para el cumplimiento de una obligación legal.

La supresión no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, prevalezcan razones de interés público para el tratamiento de datos cuestionado, o los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el responsable o encargado del tratamiento y el titular de los datos.
La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.

Artículo 22. Derecho a la Portabilidad

Cuando se traten datos personales por vía electrónica o medios automatizados, el titular de datos podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable conforme a la reglamentación técnica.
No resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular de datos.

Este derecho no procederá cuando:

1. Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable debidamente demostrada sobre el responsable o encargado del tratamiento;
2. Vulnere la privacidad de otro titular de datos;
3. Vulnere las obligaciones legales del responsable o encargado del tratamiento,
4. Impida que el responsable y/o encargado del tratamiento proteja sus derechos, su seguridad o sus bienes, o los del titular de datos o tercero,
5. Se trate de datos que ya hayan sido anonimizados por el responsable del tratamiento.

Artículo 23. Derechos ante decisiones automatizadas o semiautomatizadas.

El titular de datos tiene derecho a solicitar la revisión por una persona humana de las decisiones tomadas sobre la base del tratamiento automatizado o semiautomatizado que afecten a sus intereses, incluidas las decisiones encaminadas a definir sus aspectos personales, profesionales, de consumo, de crédito, de su personalidad u otros. Asimismo, derecho a expresar su punto de vista y a impugnar la decisión.

El Responsable de tratamiento debe proporcionar, siempre que se le solicite, información clara, completa y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada o semiautomatizada, con observancia de secretos comerciales e industriales. Debe adoptar las medidas adecuadas para salvaguardar los derechos del Titular de los datos.

Este derecho no suprime ni sustituye el ejercicio de otros derechos que puedan tener lugar.

Artículo 24. Bases legales para el tratamiento de datos personales

El tratamiento de datos personales sólo podrá realizarse si se cumple al menos una de las siguientes condiciones:

1. el titular de los datos otorgue su consentimiento, conforme lo dispuesto en el artículo 25;
2. el cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento;
3. el tratamiento y uso compartido de los datos necesarios y proporcionales, por parte de la de los poderes del Estado, para el ejercicio de sus funciones propias, la ejecución de las políticas públicas previstas en leyes y reglamentos o sustentadas en convenios interinstitucionales, sujeto a lo dispuesto en el Título V, Capítulo I de esta Ley;
4. el tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público;
5. cuando sea necesario para la ejecución de un contrato o trámites preliminares relacionados con un contrato del que el titular sea parte, a solicitud de este;
6. para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales,
7. cuando sea necesario para atender los intereses legítimos del responsable o de un tercero, siempre que sobre dichos intereses no prevalezcan los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Este numeral no resultará aplicable a los tratamientos de datos personales realizados por la administración pública.

Artículo 25. Condiciones para el consentimiento

Si la base legal para tratamiento de datos es el consentimiento, este deber ser previo, libre, específico, informado e inequívoco, para una o varias finalidades determinadas, ya sea mediante una declaración o una clara acción afirmativa, así como cumplir con el derecho a la información.

Siempre que haya cambios en la finalidad del tratamiento de datos personales, el responsable deberá volver a solicitar al titular su consentimiento.

Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocar en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos. Dicha revocación no tendrá efectos retroactivos.

Para el tratamiento de datos sensibles se requiere el consentimiento salvo las excepciones establecidas por ley.

En todos los casos, el responsable del tratamiento tiene la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

Artículo 26. Consentimiento de niños, niñas y adolescentes

En el tratamiento de datos personales de una niña, niño o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la Convención Sobre Los Derechos Del Niño y demás instrumentos internacionales firmados y ratificados por la República del Paraguay y las leyes nacionales

El tratamiento de los datos personales de los adolescentes podrá fundarse en su consentimiento a partir de los catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad, guarda o tutela, para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. El tratamiento de los datos de los niños y niñas de hasta trece años, fundado en el consentimiento, sólo será lícito si consta el del titular de la patria potestad, guarda o tutela, con el alcance que determinen los titulares de la patria potestad, guarda o tutela.

El responsable y encargado deberán realizar esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad, guarda o tutela, o bien, por el adolescente directamente atendiendo a su edad de acuerdo con la legislación vigente, teniendo en cuenta la tecnología disponible.

Se prohíbe realizar el tratamiento de datos personales de niños, niñas y adolescentes en los juegos, aplicaciones, desarrollos e innovaciones tecnológicas, u otras actividades afines que involucren información personal, más allá de lo estrictamente necesario para la realización de la actividad.

La información sobre el consentimiento y tratamiento de datos a que se refiere este artículo debe ser brindada de forma simple, clara y accesible, considerando las características físico-motoras,

perceptivas, sensoriales, intelectuales y mentales del usuario, con el uso de recursos audiovisuales cuando corresponda.

Es tarea del Estado y de las entidades educativas proveer información y capacitar a niñas, niños y adolescentes sobre los eventuales riesgos a los que se enfrentan respecto del tratamiento indebido de sus datos personales, sobre el uso responsable y seguro de sus datos personales, sobre su derecho a la privacidad y a la autodeterminación informativa, y sobre el respeto de los derechos de los demás.

Artículo 27. Interés legítimo

El interés legítimo del responsable o del tercero al que se comunique los datos, constituye una base jurídica para el tratamiento de datos personales, siempre que no prevalezcan los derechos y libertades fundamentales del titular del dato.

Para fundamentar la existencia de un interés legítimo que justifique la necesidad del tratamiento de datos personales, el Responsable de tratamiento debe realizar un análisis detallado, previo y documentado, que incluya el contexto y las circunstancias en las que se llevará a cabo el tratamiento y el nivel de riesgo que implica. En este caso deberá reforzarse el respeto del principio de minimización de datos y su tratamiento deberá acotarse sobre la base de criterios expresos de proporcionalidad y razonabilidad.

El tratamiento fundado en el interés legítimo deberá darse siempre en el marco de una relación pertinente y apropiada entre el titular de datos y el responsable, y ser conforme a las expectativas razonables del titular.

Se considera que existe interés legítimo en los siguientes casos:

A. Para prevenir el fraude.
B. Garantizar la seguridad de la red y de la información del Responsable o Encargado, así como de los servicios proporcionados a través de esos sistemas o redes de información.
C. Compartir datos personales en el marco de las operaciones normales de negocio dentro de un mismo grupo empresarial o entre entidades afiliadas a un mismo organismo central.
D. Actividades de promoción del responsable del tratamiento.

El responsable del tratamiento deberá tratar los datos estrictamente necesarios y adoptar medidas para garantizar la transparencia de dicho tratamiento, informando al titular cuál es el interés legítimo que persigue.

En el marco de los procesos de control del cumplimiento de las disposiciones de la presente Ley, la Autoridad de Control podrá requerir al Responsable de tratamiento, el análisis previo que fundamenta el tratamiento de los datos personales para la satisfacción de un interés legítimo, y el Responsable de tratamiento deberá ser capaz de demostrar la existencia del interés legítimo, la necesidad de recolectar o tratar los datos en cada caso, y los criterios de razonabilidad y proporcionalidad considerados para acotar dicho tratamiento, teniendo para sí la carga de la prueba, observando secretos comerciales e industriales.

El titular tendrá derecho a oponerse en cualquier momento al tratamiento de sus datos personales basado en el interés legítimo del responsable.

Artículo 28. Tratamiento de datos sensibles

A fin de evitar el tratamiento con fines discriminatorios, ilícitos o abusivos queda prohibido el tratamiento de datos personales sensibles salvo que:

1. El titular haya dado su consentimiento para el tratamiento de dichos datos personales,
2. El tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
3. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad social;
4. El tratamiento sea necesario para proteger intereses vitales del titular o, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento y sus representantes legales no lo puedan realizar en tiempo oportuno;
5. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares;
6. El tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial, o en procesos administrativos o arbitrales; así como los órganos de investigación de justicia;
7. El tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios;
8. Se realice en el marco de asistencia humanitaria en casos de desastres naturales;
9. El tratamiento sea necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. Los datos deberán estar anonimizados, en la medida de lo posible;
10. El tratamiento y uso compartido de los datos necesarios y proporcionales, por parte de los poderes del Estado, para el ejercicio de sus funciones propias, la ejecución de las políticas públicas previstas en leyes, sujeto a lo dispuesto en el Título V, Capítulo I de esta Ley.

Se prohíbe la comunicación o uso compartido entre responsables del tratamiento de datos personales sensibles relacionados con la salud con el fin de obtener una ventaja económica.

Se prohíbe a los operadores de planes de salud privados el tratamiento de datos de salud para la práctica de selección de riesgos al contratar cualquier modalidad, así como al contratar y excluir beneficiarios.

En todos los casos, el tratamiento deberá realizarse respetando los principios del secreto profesional, la normativa específica y los principios y disposiciones establecidas en la presente ley.

Artículo 29. Tratamiento de datos de información crediticia

La protección de datos crediticios, la regulación de la actividad de recolección y el acceso a datos de información crediticia, así como la constitución, organización, funcionamiento, derechos, obligaciones y extinción de las personas jurídicas que se dediquen a la obtención y provisión de información crediticia se regirán por la ley específica vigente al respecto.

Salvo las funciones y atribuciones expresamente asignadas al Banco Central del Paraguay, las demás requeridas para la implementación de la ley que regula los datos crediticios, serán ejercidas por la Autoridad de Control y supervisión de la presente ley.

La presente ley será de aplicación supletoria para las cuestiones no previstas en la ley que regula los datos crediticios.

Artículo 30. Tratamiento de datos con fines de publicidad

Cuando los datos personales sean utilizados para perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en fuentes de acceso público, hayan sido obtenidos con el consentimiento de los propios titulares o corresponda a un interés legítimo del responsable conforme a lo establecido en la presente ley.

En toda comunicación con fines de publicidad que se realice por correo postal, teléfono, correo electrónico, Internet u otro medio de comunicación que permita la tecnología en el futuro, el responsable o encargado del tratamiento debe implementar medidas razonables que informen al titular de los datos la posibilidad de ejercer los derechos previstos en la presente Ley.

El titular podrá en cualquier momento solicitar la supresión o bloqueo de sus datos de las bases de datos a los que se refiere el presente artículo. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, el responsable cumplirá con lo establecido en el artículo 20 del derecho de oposición.

Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición al mismo.

Artículo 31. Tratamientos con fines de videovigilancia

Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicas o de infraestructuras vinculadas al transporte u otro tipo de infraestructura crítica, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

Los datos serán suprimidos en un plazo máximo de 6 meses desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas (setenta y dos) desde que se tuviera conocimiento de la existencia de la grabación de estos hechos, sin perjuicio de las facultades de investigación de las autoridades competentes en el marco de una investigación abierta.

Se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

Artículo 32. Tratamiento de datos personales por el Estado

El tratamiento de los datos personales podrá llevarse a cabo por los organismos y entidades del Estado con el objetivo de cumplir con atribuciones legales, siempre que:

1. En ejercicio de sus competencias, realicen el tratamiento de datos personales, aportando información clara y actualizada sobre la disposición legal, finalidad, procedimientos y prácticas utilizadas para realizar estas actividades;
2. Designe un Oficial de Protección de Datos de conformidad con el art. 51, numeral 1 de esta Ley;

Los servicios notariales que se realicen por delegación del Poder del Estado tendrán el mismo tratamiento que las personas jurídicas de derecho público, en los términos de este Capítulo.

Las empresas públicas y las sociedades de capital mixto, cuando se encuentren operando políticas públicas y en el ámbito de su implementación, tendrán el mismo tratamiento que se le da a los órganos y entidades de la Administración Pública, en los términos de este Capítulo.

La Autoridad de Control podrá solicitar, en cualquier momento, a los órganos y entidades de la Administración Pública para la realización de operaciones de tratamiento de datos personales, información específica sobre el alcance y naturaleza de los datos, garantías y demás detalles del tratamiento realizado.

La Autoridad de Control podrá establecer reglas complementarias para las actividades de comunicación y uso compartido de datos personales.

Artículo 33. Cesión de datos personales entre instituciones públicas

Será lícita la comunicación de datos personales entre instituciones públicas, en la medida en que:

1. La institución pública responsable de la base de datos haya obtenido los datos en ejercicio de sus funciones y competencias legalmente atribuidas;
2. El tratamiento por parte de la institución pública que recibe la base de datos sea necesario para el cumplimiento de sus funciones legales y la finalidad de dicho tratamiento de datos se encuentre dentro del marco de sus competencias,
3. Los datos involucrados sean adecuados, proporcionales y no excedan el límite de lo necesario con relación a esta última finalidad.
4. El titular de los datos sensibles haya dado su consentimiento o se apliquen las excepciones establecidas en el artículo 28.

El uso compartido de datos personales por parte de la Administración Pública debe servir para fines específicos, para la ejecución de políticas públicas y atribución legal por parte de organismos y entidades públicas, respetando los principios de protección de datos personales enumerados en el Título II de esta Ley.

Los datos deben mantenerse en un formato interoperable y estructurado de uso compartido, con miras a la implementación de políticas públicas, la prestación de servicios públicos, la descentralización de la actividad pública y la difusión y acceso de la información al público en general.

Artículo 34. Cesión de datos personales a entidades privadas

Se prohíbe a la Administración Pública transferir a entidades privadas datos personales contenidos en bases de datos de las que sea responsable o tenga acceso, salvo que

1. En los casos necesarios de ejecución descentralizada de una función pública legalmente atribuida que requiera la comunicación o cesión, o para la satisfacción de un interés público directamente comprometido, debiéndose garantizar en estos casos que el acceso se restrinja a lo estrictamente necesario para la finalidad y sea proporcional a la misma;
2. Cuando exista una disposición de rango legal que disponga la comunicación o cesión

En todos los casos, se deberán respetar los principios de protección de datos personales enumerados en el Título II de esta Ley.

La Autoridad de Control reglamentará en coordinación con el Organismo público competente en la materia, las condiciones en que procede esta comunicación y sus limitaciones. En todos los casos, la comunicación se respaldará en convenios aprobados previamente por la Autoridad de Control.

Artículo 35. Tratamiento de datos en el ámbito de la función estadística pública

El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en la presente ley.

Se dispondrán de medidas técnicas y organizativas, para garantizar el respeto del principio de minimización de los datos personales.

Artículo 36. Tratamiento de datos con fines de archivo en interés Público por parte Administraciones Públicas

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en la presente ley y a las leyes específicas que salvaguarden los derechos de los titulares.

Artículo 37. Tratamiento de datos de naturaleza penal, infracciones y sanciones a

El tratamiento de datos personales relativos a hechos punibles, así como a procedimientos y medidas cautelares y de seguridad conexas, se regirán por la ley respectiva.

El tratamiento de datos relativos a infracciones y sanciones administrativas, se regirá por su ley respectiva.

Se dispondrán de medidas técnicas y organizativas, para garantizar el respeto del principio de minimización y demás principios y disposiciones de protección de datos personales.

Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas sólo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Artículo 38. Del tratamiento de datos personales con fines de defensa nacional o s pública

El tratamiento de datos personales con fines de defensa nacional, represión de delitos o seguridad pública por parte de las fuerzas armadas, organismos policiales e inteligencia, y el Ministerio Público, queda limitado a aquellos casos en los que resulten necesarios y proporcionales para el estricto cumplimiento de las competencias legalmente asignadas a aquéllos.

En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

Artículo 39. Del principio de transparencia gubernamental y la protección de datos personales.

La obligación de publicidad de actos de organismos y entidades del estado deberá tener en cuenta los principios de protección de datos personales establecidos en la presente ley y, en particular, el principio de minimización. Procederá la publicación y difusión de datos personales cuya inclusión sea necesaria y proporcional a la finalidad de transparencia perseguida por medio de la publicidad en el caso concreto. Los datos personales que excedan de dicha finalidad, o cuya publicación no fuere necesaria, deberán ser

excluidos o tachados de los actos o documentos a ser publicados. Está prohibida la publicación de datos sensibles.

El derecho de acceso a la información obrante en fuentes públicas podrá ser denegado o limitado, cuando tal medida resultase necesaria para evitar un perjuicio concreto a la protección de uno de los intereses privados inherentes a: (a) la protección de los datos personales, de conformidad con lo establecido en la presente ley y de acuerdo con el trámite previsto en el presente artículo; (b) la libertad y el secreto de la correspondencia; (c) los intereses económicos y comerciales de una persona física o jurídica, incluidos la propiedad intelectual, los derechos de autor y los secretos comerciales.

Artículo 40. Medidas para el cumplimiento de la responsabilidad activa

Los responsables determinarán las medidas técnicas y organizativas, adoptadas de forma proactiva para el cumplimiento de las disposiciones de la presente ley.

Las medidas adoptadas deben ser útiles, proporcionales a las modalidades y finalidades del tratamiento de datos, su naturaleza, el ámbito, el contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de su titular.

Deben contemplar, como mínimo:

1. La implementación de procedimientos para atender el ejercicio de los derechos por parte de los titulares de los datos;
2. La revisión periódica de las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
3. La implementación de sistemas de administración de riesgos asociados al tratamiento de datos personales.
4. La realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas.

Las medidas deben ser aplicadas de modo que permitan su demostración ante el requerimiento de la Autoridad de Control. En caso de denuncias, la carga de la prueba quedará a cargo del responsable del tratamiento.

Se debe adoptar una política de protección de datos o adherirse a mecanismos de autorregulación vinculantes, que serán valorados por la Autoridad de Control para verificar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

El responsable deberá valorar si procede la realización de la evaluación de impacto en la protección de datos y de la consulta previa a que se refiere la presente ley.

Artículo 41. Protección de datos desde el diseño y por defecto

El responsable del tratamiento debe aplicar, desde el diseño para el desarrollo de productos y servicios, medidas técnicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos

establecidos en la presente Ley. Las medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares.

El responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas físicas.

Artículo 42. Mecanismos de autorregulación vinculantes

La Autoridad de Control promoverá y ponderará de manera positiva la elaboración de mecanismos de autorregulación vinculantes, que tengan por objeto contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas del tratamiento de datos que se realice, así como el efectivo ejercicio y respeto de los derechos del titular de los datos.

Los mecanismos de autorregulación vinculantes podrán consistir en códigos de conducta, de buenas prácticas, normas corporativas vinculantes, sellos de confianza, certificaciones u otros mecanismos que coadyuven a contribuir a los objetivos señalados. Los códigos de conducta pueden dotarse de mecanismos de resolución extrajudicial de conflictos.

Los Responsables o Encargados de tratamiento pueden adherirse a ello de manera voluntaria.

Las asociaciones u otras entidades representativas de categorías de responsables o encargados del tratamiento podrán adoptar mecanismos de autorregulación vinculantes que resulten obligatorios para todos sus miembros.

Los mecanismos de autorregulación vinculantes serán presentados para su homologación ante la Autoridad de Control, la cual determinará si estos se adecuan a las disposiciones de la presente ley y, en su caso, los aprobará o indicará las correcciones que estime necesarias para su aprobación.

Los mecanismos de autorregulación vinculantes que resulten aprobados serán registrados y dados a publicidad por la Autoridad de Control.

Artículo 43. Seguridad del tratamiento

Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán

medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

1. la seudonimización y el cifrado de datos personales;
2. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
3. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
4. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

El Responsable y el Encargado de tratamiento de datos personales deben evidenciar que las medidas adoptadas e implementadas evitan la materialización de los riesgos identificados.

La adhesión a un código de conducta o a un mecanismo de certificación aprobado por la Autoridad de Control podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el presente artículo.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales sólo pueda tratar dichos datos siguiendo instrucciones del responsable.

Artículo 44. Notificación de un incidente de seguridad del tratamiento de los dato la Autoridad de Control

En caso de que ocurra un incidente de seguridad de los datos personales, el responsable del tratamiento la notificará a la Autoridad de Control sin dilación indebida dentro de las 72 horas (setenta y dos) después de que haya tenido conocimiento de aquel. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas (setenta y dos), deberá ir acompañada de indicación de los motivos de la dilación, justificando de manera objetiva y fundada

El encargado del tratamiento notificará dentro del plazo legal al responsable del tratamiento el incidente de seguridad de los datos personales del que tenga conocimiento.

La notificación deberá, como mínimo:

1. Describir la naturaleza del incidente de seguridad de los datos personales, el número aproximado de titulares de datos afectados, y las categorías de datos afectados;
2. Comunicar el nombre y los datos de contacto del Oficial de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
3. Describir las posibles consecuencias de la violación de la seguridad de los datos personales;

4. Describir las medidas adoptadas y a adoptar por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. Asimismo, se podrá solicitar un plazo adicional a consideración de la Autoridad de Control, en caso de que existan razones fundadas para ello.

El responsable del tratamiento documentará cada incidente de seguridad de riesgo que afecte a los derechos de los titulares de datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la Autoridad de Control verificar el cumplimiento de lo dispuesto en el presente artículo.

No será necesaria la notificación de los incidentes de seguridad en los casos en que sea improbable que constituya un riesgo para los derechos y libertades de los titulares de datos. En la reglamentación se establecerán parámetros que permitan considerar este tipo de incidentes.

Artículo 45. Comunicación de un incidente de seguridad de los datos personales a

Cuando sea probable que la violación de la seguridad de los datos personales entrañe riesgo para los derechos y libertades de las personas físicas conforme a la reglamentación de la ley, el responsable del tratamiento la comunicará al titular sin dilación indebida.

La comunicación al titular contemplada en el presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 47, numeral 2, 3 y 4.

La comunicación al Titular a que se refiere el presente artículo no será necesaria si se cumple alguna de las condiciones siguientes:

1. el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
2. el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el riesgo para los derechos y libertades del titular del dato a que se refiere el presente artículo;
3. suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida similar por la que se informe de manera igualmente efectiva a los titulares.

Cuando el responsable todavía no haya comunicado al titular el incidente de seguridad de los datos personales, la Autoridad de Control, una vez considerada la probabilidad de que tal violación entrañe un riesgo, podrá exigirle que lo haga o podrá decidir que dicha comunicación no es necesaria si cumple alguna de las condiciones mencionadas en el tercer párrafo de este artículo.

Artículo 46. Evaluación De Impacto

Cuando el responsable del tratamiento prevea realizar algún tipo de tratamiento de datos que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un riesgo de afectación a los derechos de los titulares de los datos amparados en la presente Ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.

La evaluación de impacto relativa a la protección de los datos es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la Autoridad de Control:
a- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b- Tratamiento de datos sensibles a gran escala;
c- Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La evaluación de impacto debe incluir, como mínimo:

1. Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
2. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad;
3. Una evaluación de los riesgos para la protección de los datos personales de los titulares de los datos a que se refiere el numeral 1.
4. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, y para demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas que pudieran verse potencialmente afectadas.

La Autoridad de Control podrá solicitar a las Instituciones Públicas que elaboren y publiquen informes sobre el impacto de la protección de datos personales y sugerir la adopción de normas y buenas prácticas para el tratamiento de datos personales.

Artículo 47. Consulta Previa

Cuando una evaluación de impacto evidencie que el tratamiento entraña un alto riesgo, el Responsable de tratamiento debe informar de esta circunstancia a la Autoridad de Control.

El informe debe incluir, como mínimo:

1. Las responsabilidades respectivas del responsable del tratamiento y los encargados del tratamiento, en particular en caso de tratamiento de datos dentro de un mismo grupo económico;

2. Los fines y medios del tratamiento previsto;
3. Las medidas y garantías establecidas para minimizar los riesgos identificados y proteger los datos personales de sus titulares de conformidad con la presente Ley;
4. En su caso, los datos de contacto del Oficial de protección de datos;
5. La evaluación de impacto relativa a la protección de datos.
6. Cualquier otra información que solicite la Autoridad de Control.

El Responsable de tratamiento no podrá iniciar el tratamiento de datos hasta tanto la Autoridad de Control se pronuncie sobre el informe.

La Autoridad de Control deberá, en un plazo de 30 (treinta) días hábiles desde la consulta, asesorar por escrito al responsable o encargado, de conformidad con las funciones establecidas en el artículo 66 de la presente ley. Estos plazos podrán suspenderse hasta que la Autoridad de Control haya obtenido la información solicitada a los fines de la consulta.

Artículo 48. Oficial de Protección de Datos

Los responsables y encargados del tratamiento deben designar un Oficial de Protección de Datos en cualquiera de los siguientes supuestos:

1. Cuando revistan el carácter de autoridades u organismos públicos;
2. Se realice tratamiento a gran escala de datos sensibles o de datos personales como parte de la actividad principal del responsable o encargado del tratamiento;
3. las actividades principales del responsable o del encargado que consistan en operaciones de tratamiento que, debido a su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares de datos a gran escala.

El Oficial de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones atribuidas en la presente ley.

Cuando los responsables y encargados del tratamiento no se encuentren obligados a la designación de un Oficial de Protección de Datos de acuerdo con lo previsto en este artículo, pero decidan designarlo de manera voluntaria o por orden expresa de la autoridad de control, el Oficial de Protección de Datos designado tendrá las funciones previstas en la presente ley.

El responsable y el encargado del tratamiento publicarán los datos de contacto del Oficial de protección de datos y los comunicarán a la Autoridad de Control.

La reglamentación establecerá otros aspectos relativos al oficial de protección de datos

Artículo 49. Posición del Oficial de protección de datos.

El responsable y el encargado del tratamiento garantizarán que el Oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

El responsable y el encargado del tratamiento respaldarán al Oficial de protección de datos en el desempeño de las funciones mencionadas en el artículo 53, facilitando los recursos necesarios para dichas funciones y el acceso al tratamiento, y para el mantenimiento de sus conocimientos especializados.

El responsable y el encargado del tratamiento garantizarán que el Oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El Oficial de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Los titulares de datos podrán ponerse en contacto con el Oficial de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo de la presente Ley.

El Oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con la legislación nacional.

El Oficial de protección de datos podrá desempeñar otras funciones dentro o fuera de la empresa, institución u organización en la que cumpla este rol, siempre que ello no genere conflictos de intereses de ningún tipo, debiendo establecer e implementar mecanismos para detectar y prevenir los conflictos de intereses.

Artículo 50. Funciones del Oficial de Protección de Datos

El Oficial de Protección de Datos tiene las siguientes funciones, sin perjuicio de otras que se le asignen especialmente:

1. Actuar como interlocutor del responsable o encargado del tratamiento ante la Autoridad de Control.
2. Informar y asesorar a los responsables y encargados del tratamiento, así como a sus empleados, de las obligaciones que tienen, derivadas de la normativa de protección de datos;
3. Promover y participar en el diseño y aplicación de una política de protección de datos que contemple los tratamientos de datos que realice el responsable o encargado del tratamiento;
4. Supervisar el cumplimiento de la presente Ley y de la política de protección de datos de un organismo público o empresa privada;
5. Asignar responsabilidades, concientizar y formar al personal, y realizar las auditorías correspondientes;
6. Brindar el asesoramiento que se le solicite para hacer una evaluación de impacto relativa a la protección de datos, cuando entrañe un riesgo de afectación para los derechos de los titulares de los datos, y supervisar luego su aplicación;
7. Cooperar y actuar como referente ante la Autoridad de Control para cualquier consulta sobre el tratamiento de datos efectuado por el responsable o encargado del tratamiento.

8. Recibir las comunicaciones y los reclamos de los titulares, y tramitarlos conforme a la ley.
9. Ejecutar las demás atribuciones determinadas por el responsable o encargado o establecidas en normas complementarias.

El Oficial de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Artículo 51. Deberes del Responsable del Tratamiento

Los Responsables de tratamiento deben cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, las normas reglamentarias y otras que rijan su actividad:

a) Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y las normas reglamentarias,;

b) Garantizar a la persona Titular de los datos, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos,

c) Cumplir con el deber de informar a la persona Titular de los datos sobre la finalidad de la recolección y sus derechos;

d) Tratar los datos personales bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos y exactos;

f) Tramitar las solicitudes presentadas por la persona Titular de los datos, y responderlas de manera completa y oportuna;

g) Notificar en el plazo de ley a la Autoridad de Control y a las personas Titulares de los datos los incidentes de seguridad ocurridos, de acuerdo al artículo 48 de la presente Ley;

i) Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado de tratamiento;

j) Verificar que los Encargados de tratamiento, o quienes estos subcontraten, ofrezcan garantías suficientes para realizar el tratamiento de datos personales conforme a los requisitos de la presente Ley y garanticen la protección de los derechos de la persona Titular de los datos; dicha verificación debe realizarse con anterioridad a la contratación o realización de otro acto jurídico que lo vincule con el Encargado de tratamiento;

k) En caso de que corresponda, designar un Oficial de Protección de Datos.

l) Cumplir las órdenes o requerimientos que imparta la Autoridad de Control.

l) Si el tratamiento de datos consiste en una cesión, el Responsable de tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el cedente. Ambos responden por la observancia de aquellas ante la Autoridad de Control y la persona Titular de los datos de que se trate. En cualquier caso, pueden ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño.

Artículo 52. Deberes del Encargado del Tratamiento

El encargado del tratamiento se encuentra limitado a llevar a cabo sólo aquellos tratamientos de datos encomendados por el responsable del tratamiento. Los datos personales objeto de tratamiento no pueden aplicarse o utilizarse con un fin distinto al que figure en el contrato ni ser cedidos a otras personas, ni aún para su conservación, salvo autorización expresa del responsable del tratamiento.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo a la legislación nacional, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de titulares de datos, y las obligaciones y derechos del responsable y encargado.

El encargado asumirá las mismas funciones establecidas en la ley para el Responsable, que le resulten aplicables.

Artículo 53. Sub Encargado de Tratamiento

El encargado puede suscribir un contrato para subcontratar servicios que impliquen el tratamiento de datos solamente cuando exista una autorización expresa del responsable del tratamiento. En estos casos el subcontratado asume el carácter de responsable en los términos y condiciones previstos en esta Ley.
En los casos en los que el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos que lleve a cabo conforme a lo estipulado en el contrato, se le reputará la calidad de responsable del tratamiento en los términos y condiciones previstos en la presente Ley.

Los contratos previstos en este artículo deberán estipular mínimamente el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento de datos, el tipo de datos personales, las categorías de titulares de los datos y las obligaciones y responsabilidades del responsable y encargado del tratamiento.

Una vez cumplida la prestación contractual, los datos personales tratados deben ser destruidos, salvo disposiciones expresas al respecto en la ley.

Artículo 54. Representantes de responsables o encargados del tratamiento no est Paraguay

Cuando sea de aplicación el artículo 2, inciso b), c) y d) el responsable o el encargado del tratamiento designará por escrito un representante en la República del Paraguay.

La obligación del presente artículo no será aplicable cuando:

1. el tratamiento sea ocasional, que no incluyan el manejo a gran escala de datos sensibles y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o
2. el tratamiento sea realizado por organismos públicos extranjeros.

El responsable o encargado comunicará a la Autoridad de Control los datos de contacto de su representante. Las notificaciones o intimaciones serán realizadas en el domicilio del representante y serán válidas como si fueran hechas al responsable o al encargado.

El Representante podrá responder a la solicitud hecha por el Titular del dato así como a la de la Autoridad de Control.

La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 55. Reglas generales para las transferencias internacionales de datos per

Las transferencias de datos personales fuera del territorio nacional, incluidas las transferencias ulteriores desde el tercer país u organización internacional a otro tercer país u otra organización internacional, se podrá realizar en cualquiera de los siguientes supuestos:

1. El país u organización internacional o supranacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales;
2. El exportador ofrezca garantías apropiadas al tratamiento de los datos personales, en cumplimiento de las condiciones mínimas y suficientes establecidas en esta ley.
3. Excepciones previstas en la ley.

Artículo 56. Carácter adecuado del país u organismo receptor

El nivel de protección de datos del país extranjero o de la organización internacional o supranacional a que se refiere el numeral 1 del art. 57 de esta Ley, será evaluado por la Autoridad de Control, a pedido de parte interesada o de oficio, teniendo en cuenta:

a) las normas generales y sectoriales de la legislación vigente en el país de destino o en la organización internacional; incluyendo las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;
b) observancia de los principios generales de protección de datos personales y derechos de los titulares previstos en esta Ley;
c) la existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales;
d) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales están sujeta una organización internacional; y,
e) otras circunstancias específicas relacionadas con la transferencia.

La Autoridad de Control publicará en su sitio web la lista de países y organizaciones internacionales que garanticen niveles adecuados de protección de datos personales.

Artículo 57. Transferencias mediante garantías apropiadas

Las garantías apropiadas de conformidad al numeral 2 del artículo 57 podrán ser aportadas, por:

a. un instrumento jurídicamente vinculante y exigible entre las autoridades o instituciones públicas de Paraguay y otro país que contengan los principios, derechos y obligaciones establecidos en esta ley;
b. Acuerdos o convenios que reconozcan los principios, derechos y obligaciones establecidos en esta ley, que pueden adoptar alguna de las siguientes formas:

    a. Cláusulas tipo de protección de datos aprobadas por la Autoridad de Control;

    b. Normas corporativas vinculantes que hayan sido aprobadas por la Autoridad de aplicación y que se apliquen a todos los miembros de un grupo económico en los términos que establece esta ley;

    c. Código de conducta aprobado, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los titulares de datos, o;

    d. Un mecanismo de certificación aprobado por la Autoridad de Control, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares de datos.

El receptor de los datos personales asume las mismas obligaciones que corresponden al responsable del tratamiento que transfirió los datos personales.

Artículo 58. Excepciones

En ausencia de una decisión de adecuación o de garantías apropiadas establecidos en el numeral 2 del artículo precedente, la transferencia se podrá realizar con las debidas salvaguardas adicionales si se cumple una de las condiciones siguientes:

1. La transferencia sea necesaria para la cooperación jurídica internacional entre órganos de inteligencia pública, investigación y enjuiciamiento, de conformidad con los instrumentos del derecho internacional;
2. La transferencia se encuentre prevista en esta ley u otras leyes, convenios o tratados internacionales en los que Paraguay sea parte siempre y cuando no sean contrarias a las disposiciones de esta ley;
3. La transferencia sea necesaria, para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
4. La transferencia sea necesaria para proteger la vida o la seguridad física del titular o de un tercero;
5. El titular del dato haya dado su consentimiento expreso, con información previa sobre el carácter internacional de la operación, distinguiéndose claramente de otros fines.

Artículo 59. Prueba del cumplimiento de las obligaciones en materia de transferencias internacionales

A efectos de demostrar que la transferencia internacional se ha realizado conforme a lo que establece la presente Ley, la carga de la prueba recae, en todos los casos, en el responsable del tratamiento que transfiere.

Artículo 60. Autoridad de control y supervisión. Naturaleza jurídica.

Créase la Agencia de Protección de Datos Personales como una unidad dentro de la estructura orgánica del Ministerio de Tecnologías de la Información y Comunicación (MITIC), con el rango de Dirección General, que se constituye en la Autoridad de control y supervisión de las disposiciones de la presente ley.

La Agencia será titular de las competencias atribuidas en la ley, con imputación funcional de forma permanente, exclusiva y regular, constituyendo una unidad desconcentrada en el Ministerio de Tecnologías de la Información y Comunicación (MITIC), con facultades de decisión, acción, supervisión, control y demás atribuidas en la ley, actuando conforme a los principios en ella establecidos.

El Director General tendrá dedicación exclusiva en su función, y ejercerá sus funciones legalmente atribuidas con plena independencia y no estará sujeto a instrucciones respecto de estas.

Compete a la Agencia de Protección de Datos Personales el ejercicio de acciones ante las autoridades nacionales e internacionales y organismos privados o personas vinculadas a la protección de los datos. Le corresponde así también la asistencia técnica a cualquier institución que lo solicite para la protección de datos personales.

La Autoridad de Control deberá contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

Transcurrido el periodo inicial de la entrada en funciones de la Agencia de Protección de Datos Personales y atendiendo al grado de alcance desplegado en su ejecución, la misma deberá ordenarse hacia la adopción de una naturaleza jurídica correspondiente a un ente descentralizado, con personería jurídica propia y plena autonomía.

La creación de la Agencia de Protección de Datos Personales dentro de la estructura orgánica del MITIC, no exime a éste de los deberes y obligaciones establecidos en la ley y su reglamentación. La Autoridad de Control tendrá sobre el MITIC iguales atribuciones y competencias que con las demás instituciones del sector público.

Artículo 61. Nombramiento del Titular de la Agencia de Datos Personales

La Agencia de Protección de Datos Personales estará bajo la titularidad de un Director General que será nombrado por Decreto del Poder Ejecutivo, a propuesta del Ministro de Tecnologías de la Información y Comunicación (MITIC), previo concurso de méritos.

Los requisitos para ser nombrado Director General de la Agencia de Protección de Datos Personales son:

1. Ser de nacionalidad paraguaya, de 30 (treinta) años de edad como mínimo;
2. Poseer título universitario de grado;
3. Contar con condiciones probadas de idoneidad, capacidad y experiencia en la materia de protección de datos personales, que aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de su cargo.
4. No podrá ser nombrado Director General quien sea accionista, miembro de la junta directiva, gerente o representante legal de una empresa dedicada a la recolección, almacenamiento y/o procesamiento de datos personales.

Artículo 62. Duración del mandato y remoción.

El Director General de la Agencia de Protección de Datos Personales durará 5 (cinco) años en su cargo, pudiendo ser designado nuevamente para periodos posteriores.

Ejercerá sus funciones con exclusividad, independencia y objetividad, quedando limitado el poder jerárquico de la máxima autoridad del MITIC para aquellos asuntos que no guarden relación con las funciones de competencia de la Autoridad de Control, excepto en caso de sumario administrativo.

El Director General cesará igualmente en el cargo por remoción en los casos de mal desempeño de sus funciones o la comisión de delitos. El sumario administrativo para comprobar las causales de remoción será tramitado conforme a lo establecido en la Ley que rige la Función Pública, ante el MITIC. Bajo ningún punto de vista podrá ser considerado un cargo de confianza a libre disposición de la administración.

El Director General responderá personalmente por las consecuencias de su gestión técnica, administrativa y financiera; y de toda decisión adoptada en contravención a las disposiciones legales y reglamentarias.

Artículo 63. Funciones y atribuciones de la Autoridad de Control

La Agencia de Protección de Datos Personales se constituye en Autoridad de Control y Supervisión de la presente ley, y cuenta con suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar su efectivo cumplimiento, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

La Autoridad de Control tendrá las siguientes funciones y atribuciones:

La Autoridad de Control tendrá las siguientes funciones y atribuciones:

1. Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales;

2. Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente Ley y de los medios legales de que disponen para la defensa de sus derechos;
3. Dictar las normas y criterios orientadores que se deben observar en el desarrollo de las actividades comprendidas por esta Ley; específicamente, dictar normas administrativas y de procedimiento relativas a las funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento de datos;
4. Tramitar los reclamos y/o denuncias interpuestos en relación con el tratamiento de datos en los términos de la presente Ley;
5. Iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento sumario, conforme a lo dispuesto en la presente ley;
6. Realizar auditorías técnicas al tratamiento de datos personales, de conformidad con la presente Ley y la reglamentación;
7. Solicitar información a las instituciones públicas y privadas, las que deberán dar respuesta en el plazo que para el efecto se establezca. Las instituciones requeridas deberán proporcionar, entre otras, información sobre el alcance y naturaleza de los datos, garantías y demás detalles del tratamiento realizado, los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se le requieran. La Autoridad deberá garantizar, cuando corresponda, la seguridad y confidencialidad de la información y elementos suministrados;
8. Imponer las sanciones administrativas que, en su caso, correspondan por violación a las normas de la presente Ley y de las reglamentaciones que se dicten en su consecuencia;
9. Homologar los mecanismos de autorregulación vinculantes o códigos de conductas y supervisar su cumplimiento;
10. Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas;
11. Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos;
12. Crear mecanismos de certificación en materia de protección de datos, a fin de aportar las garantías establecidas;
13. Evaluar el carácter adecuado del país u organismo receptor en la transferencia internacional de datos;
14. Solicitar información a los Oficiales de Protección de Datos, en los términos de lo previsto en la presente Ley;
15. Promover acciones de cooperación con autoridades de protección de datos personales de otros países, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia, independiente o conjuntamente con el Ministro de MITIC;
16. Emitir dictamen técnico no vinculante cuando en sede administrativa o judicial deba ponderarse el derecho de acceso a la información pública y el derecho a la protección de datos personales, cuando existan dudas sobre su aplicación;
17. Publicar guías de la normativa relativa a la protección de datos personales;
18. Preparar informes anuales de gestión sobre sus actividades;
19. Asesorar en la consideración de los proyectos normativos que refieran total o parcialmente a la protección de datos personales;
20. Colaborar con la Autoridad de Aplicación del tratamiento de datos crediticios;

21. Colaborar con el Ministerio de Tecnologías de la Información y Comunicación (MITIC) en las políticas públicas, investigación y en la gestión de seguridad de la información y ciberseguridad sobre las infraestructuras de bases de datos que contengan datos personales para la adecuada protección de estos;
22. Colaborar con la Secretaría de Defensa del Consumidor (SEDECO) para la educación del consumidor en materia de datos personales;
23. Convocar instancias de múltiples partes para la colaboración, análisis, discusión y propuestas de temas de su competencia, instauración de mecanismos de gobernanza y de obtención de información por parte de sectores interesados;
24. Emitir opinión técnica o dictamen con respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales;
25. Aplicar las sanciones administrativas que, en su caso, correspondan por violación a las normas de la presente Ley y de las reglamentaciones que se dicten en su consecuencia;
26. Las demás funciones que le asigne esta ley o su Decreto Reglamentario, así como aquellas que resulten necesarias para garantizar la efectiva implementación y cumplimiento de la presente ley.

Artículo 64. De las funciones del Director o de la Directora General:

Le corresponde al Director o la Directora General de la Agencia de Protección de Datos Personales:

1. Representar a la Agencia de Protección de Datos en todos los actos en que ella intervenga,

2. Dirigir las actividades de la Agencia de conformidad a lo establecido en esta Ley y su reglamentación.

3. Controlar y hacer aplicar la presente ley.

4. Promover la concienciación del público en general y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos personales; y asesorar al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

5. Brindar información y tratar las reclamaciones de cualquier titular en relación con el ejercicio de sus derechos en virtud de la presente ley.

6. Desempeñar cualquier otra función relacionada con la protección de los datos personales.

Artículo 65. De los recursos de la Agencia de Protección de Datos Personales

Los recursos financieros de la Agencia de Protección de Datos Personales estarán constituidos por:

1. Los recursos que anualmente le sean destinados en el Presupuesto General de la Nación para el mantenimiento e incremento de sus funciones, dentro del Presupuesto del MITIC.

2. Los ingresos provenientes de las multas aplicadas en ejercicio de sus potestades sancionadoras establecidas en esta Ley.

3. Los fondos provenientes de convenios y/o acuerdos, créditos otorgados, préstamos, financiamientos, aportes, donaciones, legados, o de cualquier otro concepto, de origen nacional o internacional, siempre que no implique conflicto de interés.

Los ingresos enumerados en el inciso 2, serán depositados en una cuenta especial que se abrirá a la orden de Agencia de Protección de Datos Personales y los mismos serán destinados en forma exclusiva al cumplimiento de la presente Ley.

En ningún caso, se dispondrá de los mencionados recursos para otro objeto distinto a lo establecido en la presente Ley y sus reglamentaciones. El funcionario de la Agencia de Protección de Datos Personales o del Ministerio de Tecnologías de la Información y Comunicación que quebrante esta disposición, será personal y solidariamente responsable.

La Agencia de Protección de Datos Personales podrá conformar su propia Sub Unidad de Administración y Finanzas responsable de la administración y uso de los recursos asignados.

Artículo 66. Estándares de Interoperabilidad

La Autoridad de Control podrá disponer sobre estándares de interoperabilidad para fines de portabilidad, libre acceso a los datos y seguridad, así como sobre el tiempo de conservación de los datos, teniendo en cuenta especialmente la necesidad y la transparencia. Estos estándares deberán establecerse en coordinación con las áreas competentes del MITIC.

Artículo 67. Tutela administrativa y judicial.

El titular de los datos o su representante legal puede formular reclamos o denuncias ante la Autoridad de Control para hacer efectivos sus derechos a la protección de datos personales, en la forma y condiciones previstas en la presente ley y en su reglamentación.

La Autoridad de Control podrá asimismo iniciar procedimientos a los efectos de constatar el cumplimiento de las disposiciones de la presente Ley:

1. A instancia de la persona Titular de los datos;
2. A instancia de un tercero, asociaciones u organizaciones, siempre que exista un interés legítimo;
3. De oficio.

En los procedimientos, se aplicará lo dispuesto en la presente ley, su reglamentación y las disposiciones de la Ley N° 6715/2021 de “Procedimientos Administrativos” o equivalente, en todo cuanto resulte aplicable.

Sin perjuicio de la tutela administrativa, el titular podrá recurrir a la tutela judicial para ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de sus derechos a la protección de datos personales, conforme a la presente ley.

Artículo 68. Procedimiento para el reclamo ante la Autoridad de Control

El Titular de los datos o su representante legal pueden realizar un reclamo o denuncia, en forma gratuita, mediante cualquier medio habilitado para dicho efecto por la Autoridad de Control, expresando con claridad el contenido de su requerimiento y los preceptos de esta Ley que considere vulnerados, y acreditando haber efectuado la intimación prevista en la Ley.

La presentación debe realizarse dentro de los quince (15) días hábiles siguientes a la fecha en que se comunique la respuesta a la intimación, por parte del Responsable o Encargado de tratamiento, o en cualquier momento si el plazo establecido para el efecto hubiere vencido sin respuesta de parte del Responsable o Encargado de tratamiento. La respuesta, de haberse producido, deberá acompañar la presentación del reclamo.

Artículo 69. Procedimiento para la comprobación de faltas y aplicación de sancion

Las faltas a las disposiciones de la presente ley y sus reglamentaciones, que sean objeto de reclamo por parte del Titular de los datos, o por parte de un tercero, asociaciones u organizaciones, que acrediten un interés legítimo, o de oficio por la Autoridad de Control, deben probarse en sumario administrativo.

La instrucción del sumario será dispuesta por resolución del Director General de la Autoridad de Control, que contendrá una relación completa de los hechos, actos u omisiones que se le imputen al presunto infractor, así como la designación del Juez Instructor, que será designado, de entre quienes presten servicios en la Autoridad de Control.

La reglamentación determinará el procedimiento y plazos a seguir, incluyendo aquel con que cuenta el Juez Instructor para la presentación de su dictamen final ante el Director General y el dispuesto para la emisión de la Resolución correspondiente. Todos los demás aspectos del procedimiento, se regirán por lo establecido en la Ley N° 6715/2021 de “Procedimientos Administrativos o equivalente.

El procedimiento sumario, hasta su resolución, no tendrá una duración mayor a 90 (noventa) días corridos.

La Autoridad de Control podrá requerir informaciones a instituciones públicas, privadas y a particulares, que deberán responder dentro del plazo establecido en la reglamentación de esta ley.

Artículo 70. Medidas cautelares

Una vez iniciado el procedimiento sancionador, se podrá disponer, mediante resolución motivada, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento.

Artículo 71. Resolución de la Autoridad de Control

La Autoridad de Control podrá, mediante resolución fundada:

1. Desestimar el reclamo o denuncia presentada;
2. En caso de considerar que asiste derecho a la persona Titular de los datos, requerir al Responsable o Encargado de tratamiento que haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento a la Autoridad de Control dentro de los quince (15) días hábiles de efectuado;
3. En caso de verificarse la comisión de una falta, aplicar las sanciones previstas en la presente ley.

Artículo 72. Conductas que constituyen faltas

Se considera falta toda acción u omisión que implique incumplimiento de disposiciones establecidas en la Ley y en sus disposiciones reglamentarias, incluyendo a aquellas dictadas por la Autoridad de Control.

Las faltas se clasifican en leves y graves.

La actuación administrativa motivada en las conductas mencionadas, será independiente de las actuaciones que se lleven a cabo en instancia judicial en los casos de conductas tipificadas en el Código Penal, como también lo serán las sanciones o penas que en cada caso se apliquen.

Artículo 73: Criterios para las sanciones administrativas

Luego de ser probadas las faltas en sumario administrativo, respetando el debido proceso y las circunstancias del caso específico, las sanciones administrativas deben ser determinadas considerando los siguientes parámetros y criterios:

1. La gravedad y naturaleza de las infracciones y el daño o peligro a los intereses jurídicos tutelados en la presente Ley;
2. La buena fe del infractor o el reconocimiento o aceptación expresa que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar;
3. El grado de responsabilidad del infractor, así como la intención o negligencia en el carácter de la infracción;
4. La ventaja o beneficio económico obtenido o pretendido por el infractor en virtud de la comisión de la infracción;
5. El tamaño de la persona jurídica en términos de posición de mercado, posición económica u otros criterios considerados en la reglamentación;
6. La situación económica del infractor;

7. La reincidencia en la conducta;
8. El grado de daño;
9. La cooperación del infractor en la acción investigadora de la Autoridad de Control;
10. La adopción reiterada y demostrada de mecanismos y procedimientos internos capaces de minimizar el daño, encaminados al tratamiento seguro y adecuado de los datos;
11. La adopción de una política de buenas prácticas o código de conductas;
12. La pronta adopción de medidas correctivas;
13. La proporcionalidad entre la gravedad de la falta y la intensidad de la sanción;
14. Otros que pueda considerar la Autoridad de Control, según la naturaleza del caso..

La aplicación de los distintos tipos de sanciones podrá ser indistinta o acumulativamente.

Artículo 74. Sanciones administrativas

Las sanciones a ser aplicadas por la Autoridad de Control por las faltas comprobadas a la presente ley, podrán consistir en:

1. Apercibimiento, indicando el plazo para la adopción de medidas correctivas, en su caso;
2. Multas: desde 50 (cincuenta) hasta 50.000 (cincuenta mil) jornales mínimos para actividades diversas no especificadas en la República del Paraguay). Tratándose de infracciones cometidas en el tratamiento de datos sensibles, los montos de las sanciones podrán duplicarse;
3. Suspensión de las actividades relacionadas con el tratamiento de datos personales;

La aplicación de los distintos tipos de sanciones podrá ser indistinta o acumulativa.

La Autoridad de Control debe dar publicidad a la resolución de aplicación de sanción en su sitio web.

La Autoridad de Aplicación se encuentra facultada para dictar las normas complementarias y/o aclaratorias al presente artículo.

Artículo 75. Medidas correctivas

En caso de incumplimiento de las disposiciones previstas en la presente Ley, sin perjuicio de la sanción administrativa que se imponga, la Autoridad de Control podrá dictar medidas correctivas con el objeto de eliminar, evitar o detener los efectos de las faltas, así como también disuadir reincidencias.

Las medidas correctivas podrán consistir, entre otras, en:
1) El cese o suspensión del tratamiento, bajo determinadas condiciones o plazos;
2) La eliminación de los datos; y
3) La imposición de medidas técnicas, jurídicas, organizativas, educativas o administrativas que considere pertinentes para garantizar un tratamiento adecuado de datos personales.

Artículo 76. Pago de multas

El monto de las multas deberá ser pagado dentro del plazo establecido en la reglamentación de esta ley, así como lo referente a la falta de pago, los intereses que conlleva la falta de pago y la prescripción de la acción.

Artículo 77. Prescripción de sanciones

El plazo de prescripción de las sanciones será el previsto en la Ley N° 6715/2021 de Procedimientos Administrativos" o su equivalente.

Artículo 78. Infracción del tratamiento de los datos personales por parte de las Ins públicas

Las sanciones pecuniarias indicadas en este capítulo sólo se aplican a las personas físicas y jurídicas de derecho privado.

En caso de que la Autoridad de Control advierta un presunto incumplimiento de las disposiciones de la presente ley por parte de instituciones públicas, apercibirá y dictará una resolución estableciendo medidas correctivas que deberán ser adoptadas para que cesen o se corrijan los efectos de la infracción.

La resolución por la cual se disponga la implementación de medidas será notificada a la máxima autoridad de la institución pública en la cual haya ocurrido la falta y al titular de datos afectado, si los hay.

Sin perjuicio de lo establecido en los párrafos anteriores, la Institución pública, previo análisis de los hechos en cuestión, tomará las medidas que correspondan con respecto a los presuntos responsables, incluyendo, aunque sin limitarse a ello, la instrucción de sumario administrativo para la imposición de sanciones disciplinarias conforme al procedimiento establecido para el efecto.

Quien o quienes resulten responsables del incumplimiento de las medidas correctivas dispuestas por la Autoridad de Control de la presente Ley incurrirán en falta grave en el desempeño de sus funciones

Artículo 79. Recurso de reconsideración

Contra toda resolución o acto administrativo de carácter no reglamentario emitido por la Autoridad de Control, procede el recurso de reconsideración previsto en la Ley N° 6715/2021 de "Procedimientos Administrativos", que debe ser interpuesto ante el Director General de la Agencia de Protección de Datos Personales.

La instancia administrativa se agota con las resoluciones del Director General de la Agencia de Protección de Datos Personales. El Ministerio de Tecnologías de la Información y Comunicación no tendrá competencia para el procesamiento de solicitudes y demás trámites vinculados a derechos de protección de datos personales u otras competencias de esta Unidad.

Una vez agotada la instancia administrativa, se podrá recurrir ante el Tribunal de Cuentas.

Artículo 80.Contenido y forma de presentación

La reconsideración se formulará por escrito y contendrá en forma clara y precisa los hechos y el derecho en que se fundamenta. El plazo para su interposición y demás aspectos son los establecidos en la Ley N° 6715/2021 de “Procedimientos Administrativos” o equivalente.

Artículo 81. Acción contencioso-administrativo

La acción contencioso-administrativo deberá interponerse ante el órgano jurisdiccional competente, dentro del plazo establecido por la Ley N° 6715/2021 de “Procedimientos Administrativos”. El recurso de reconsideración y la acción contencioso-administrativo, tendrán efecto suspensivo para la aplicación de las sanciones administrativas.

Artículo 82. Disposiciones finales

La presente Ley entrará en vigor luego de transcurridos 24 (veinticuatro) meses de su publicación oficial.

Artículo 83. Reglamentación

El Poder Ejecutivo reglamentará la presente Ley en un plazo máximo de 180 (ciento ochenta) días desde su publicación oficial.

Artículo 84. Derogaciones

Quedan derogados el inciso a) y b) del artículo 3, el artículo 4, el inciso b) del artículo 20, el inciso x) del artículo 21 de la Ley Nro. 6534/2020 De Protección de Datos Personales Crediticios.

Artículo 85. Comuníquese al Poder Ejecutivo