



EXPEDIENTE ADMINISTRATIVO:

**“LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS
PERSONALES PARA LAS INSTITUCIONES QUE CONFORMAN EL
SECTOR PÚBLICO”**

AUTOR: INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA

FECHA DE APROBACIÓN POR PLENO: 02 DE ABRIL DE 2020

FECHA DE PUBLICACIÓN: 04 DE NOVIEMBRE DE 2020

SAN SALVADOR, EL SALVADOR 2020

ÍNDICE

No.	Documento	Folio
1	JUSTIFICACIÓN	1-2
2	Borrador de: <i>Lineamientos de protección de datos personales</i>	3-15
3	Reporte general del proceso LEGISLA: LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	17-34
4	Correos de comunicación electrónica referente a: <i>Seguimiento a lineamientos publicados en LEGISLA para consulta pública</i>	55
5	Lineamientos de datos personales, respuesta técnica	56-57
6	Punto SIETE de acta número doce de sesión ordinaria de fecha 30 de marzo de 2020, en la que se acordó remitir a la Unidad de Género los Lineamientos de Protección de Datos Personales, para revisión	58
7	Correos de comunicación electrónica referente a: <i>Solicitud de revisión de lineamientos desde la Unidad de Género</i>	59-60
8	Remisión de LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA INSTITUCIONES DEL SECTOR PÚBLICO, con modificaciones en cuanto al uso del lenguaje inclusivo no sexista, por parte de la Unidad de Género	61-75
9	Punto CUATRO de acta número cinco de sesión extraordinaria de fecha 2 de abril de 2020: aprobación de <i>Lineamientos de Protección de Datos Personales</i>	76
10	Invitación electrónica <i>Socialización de Lineamientos de Protección de Datos Personales con la Unidad de Formación</i>	77

11	<p>Correos de comunicación electrónica relativa a: <i>Sobre publicaciones de lineamientos de Protección de Datos Personales en el Diario Oficial</i></p> <ul style="list-style-type: none"> Cotización No. 2025: Detalle de los bienes y/o servicios a suministrar por usted(es) requerido 	78-79
12	<p>Diario Oficial de fecha miércoles 4 de noviembre de 2020, Número 220, Tomo N°429, publicación de Lineamientos Generales de Protección de Datos Personales para Instituciones Del Sector Público, pág. 23-46</p>	80-89
13	<p>ANEXO</p> <ul style="list-style-type: none"> Art. 8 de la Ley de Procedimiento Administrativos (LPA) Art. 162 de la Ley de Procedimiento Administrativos (LPA) 	79-80

JUSTIFICACIÓN

El Instituto de Acceso a la Información Pública (IAIP) es el garante de la protección de las personas respecto al tratamiento de sus datos personales y la información que les concierne; a efecto de evitar injerencias a su vida privada, intimidad y preponderar el derecho a buscar, recibir y difundir información, se emitieron los *Lineamiento para la Gestión de Solicitudes de Acceso a la Información Pública* y los *Lineamientos Generales de Protección de Datos Personales para instituciones del sector público*.

La aprobación de la anterior normativa se realizó a la luz del Art. 162 de la Ley de Procedimiento Administrativos (LPA), el que establece las directrices para la aprobación de normativa, siguiendo los pasos establecidos (1 al 7), formando a su vez el expediente administrativo (Art. 8 LPA) que contiene los documentos y actuaciones que sirvieron de antecedentes y fundamento para la formalización de los lineamiento, así como las diligencias encaminadas a su materialización; de la siguiente manera:

1. Iniciativa

Con la finalidad de armonizar los procedimientos administrativos internos en el marco de tramitación de las solicitudes de acceso a la información pública y personal, así como establecer las políticas de aplicación general que se deberán observar para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales; este Instituto en uno de sus facultades de emitir normativa respecto al derecho a la información y datos personales, y en aras de iniciar la formación del expediente, inicialmente se agregan los borradores correspondientes a los Lineamientos para la Gestión de Solicitudes de Acceso a la Información Pública y Lineamientos Generales de Protección de Datos Personales, respectivamente.

2. Recopilación de información, 3. Audiencia a los ciudadanos directamente afectados en sus derechos e intereses, 4. Participación del público y 5. Colaboración entre órganos y entes públicos

Este instituto en aras de priorizar y ponderar la participación ciudadanas, recopilación de informes y la colaboración entre entes; habilitó a través del portal

web **Consulta Ciudadana** <https://participacion.iaip.gob.sv/>, el proyecto **Legisla**, el cual nace como parte del Plan de Acción 2016 - 2018 de AGA, y tiene como objetivo, promover la transparencia y la participación ciudadana como ejes centrales de una gestión pública abierta, responsable y participativa que responda a las necesidades de la población y fomente el desarrollo sostenible del país, principalmente en el proceso de formulación de normas de las instituciones públicas.

Anudado a lo anterior a partir del 28 de febrero de dos mil veinte, se da la apertura para todas las partes interesadas (entes y ciudadanía), participen de forma activa a través de dicha plataforma, comentando y votando (a favor o en contra) cada una de las disposiciones de los Lineamientos para la Gestión de Solicitudes de Acceso a la Información Pública (<https://participacion.iaip.gob.sv/normativa/dc198f36-d142-4ad8-8469-3222bbf7574d>) y Lineamientos Generales de Protección de Datos Personales (<https://participacion.iaip.gob.sv/normativa/b7778639-24dc-4519-a89b-779921a781a5>) respectivamente, generando de esta manera una interacción directa entre el Instituto y las personas que participaron.

Cabe destacar, que dicho proyecto permitió proporcionar justificaciones técnicas a cada uno de los diferentes comentarios realizados en las disposiciones, fundando las base interpretativas a diferentes términos, ideas, y a la normativa en general.

De igual forma, la Unidad de Acceso a la Información Pública (UAIP) y la Unidad de Protección de Datos Personales (UPDP), para la ejecución de actividades que propiciaron la correcta aplicación y mecanismos de protección de la LAIP, realizaron acciones internas tales como: a) la revisión de los Lineamientos para la Gestión de Solicitudes de Acceso a la Información Pública y los Lineamientos Generales de Protección de Datos Personales y b) la socialización a unidades sobre la actualización y la nueva normativa.

Con lo anterior, este Instituto garantizó la efectiva colaboración, comunicación y participación de los entes y ciudadanos que se verían afectados con la aprobación y creación de los lineamientos en cuestión.

Asimismo, en atención a las observaciones realizadas por las jefaturas y unidades en relación a los lineamientos, se constata vía correo electrónico las comunicaciones activas que existieron.

6. Ponderación y motivación

7. Publicación

El Pleno de este Instituto, en uso de sus facultades, aprueba en el PUNTO CUATRO, del acta IAIP-A1-3.05/2020 de la sesión extraordinaria, de fecha dos de abril de 2020, los Lineamientos para la Gestión de Solicitudes de Acceso a la Información Pública y los Lineamientos Generales de Protección de Datos Personales.

Posterior a ellos se realizaron las consultas internas para la publicación de los mismo en el Diario Oficial, actuaciones que constan en el presente expediente.

En conclusión, con el propósito de brindar un fácil acceso a las actuaciones realizadas por este Instituto en el marco de aprobación de la normativa relativa a los Lineamientos para la Gestión de Solicitudes de Acceso a la Información Pública y los Lineamientos Generales de Protección de Datos Personales, se pone a disposición el presente expediente para su consulta.

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES

Considerando

I. Que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;

II. Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;

III. Que los avances tecnológicos y el progreso de la sociedad de la información ofrecen a los individuos herramientas que contribuyen a mejorar su calidad de vida. Asimismo, coadyuvan con el Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste. Por otra parte, las nuevas tecnologías facilitan ilimitadas posibilidades para transmitir un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;

IV. Que, sin embargo, un tratamiento inadecuado de esas herramientas tecnológicas y de la información personal de los habitantes puede atentar contra la privacidad, seguridad y autodeterminación informativa de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo;

V. Que se requiere un nivel uniforme y elevado de protección de las personas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras injustificadas a sus derechos y acciones desproporcionadas con el uso de sus datos personales;

VI. Que, en el tratamiento de los datos personales, es imperioso establecer un equilibrio entre los intereses de todos los actores del sector público, social y titulares involucrados, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que sean acordes con los fines perseguidos en sociedades democráticas;

VII. Observando que el artículo 6 de la Constitución establece como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el orden público, la moral, el honor, y la vida privada;

VIII. Que a su vez el acceso a la información pública está consagrado como derecho fundamental que el Estado está llamado a proteger. En este sentido, las instituciones públicas cumplen un papel fundamental en la promoción de la transparencia en su gestión, siendo los funcionarios públicos depositarios de la autoridad investida por la Nación.

IX. Que la Ley de Acceso a la Información Pública es obligatoria para los poderes públicos de la República de El Salvador, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;

X. Que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica el tratamiento de datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, responsabilidad, de información al titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transferencia;

XI. Que es de gran relevancia que las personas tengan conocimiento de la información que de ellos obra en los archivos del Sector Público a efecto de hacer uso de los derechos de acceso, rectificación, cancelación y oposición de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman;

XII. Que el Instituto de Acceso a la Información Pública es el garante de la protección de la información de carácter personal, a efecto de evitar injerencias a su vida privada, en equilibrio con los principios de Transparencia y Acceso a la Información Pública Gubernamental que se requieren para un desarrollo del Estado Democrático de Derecho;

Capítulo I: Disposiciones generales

Artículo 1.- Objeto y ámbito de aplicación

Los presentes Lineamientos establecen las políticas generales que deberán observar las dependencias y entidades de la Administración Pública para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales con el propósito de:

a. Asegurar su adecuado tratamiento e impedir su uso para finalidades distintas de aquellas que motivaron su suministro.

- b. Evitar la transferencia de datos personales que sea ilícita y lesiva para la dignidad y derechos del afectado.
- c. Instar a la Administración Pública a adoptar una cultura institucional y una concientización acerca de la importancia de poner en práctica los principios de acceso a la información pública y la transparencia, en equilibrio con el derecho a la protección de datos personales de los administrados, con las limitaciones que establece la Ley.

Artículo 2.- Elementos de los datos personales

A efecto de determinar si la información que posee un ente obligado constituye un dato personal, deberán agotarse las siguientes condiciones:

- a. Que la misma sea concerniente a una persona, identificada o identificable, y
- b. Que la información se encuentre contenida en sus archivos.

Artículo 3.- Derecho a la protección de datos personales

La protección de datos personales es el derecho autónomo, con características y dinámicas, que tiene por objeto salvaguardar el poder de disposición y el control que tiene toda persona física y jurídica con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

Se reconoce el derecho de toda persona a la protección de datos personales, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Artículo 4.- Definiciones

Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en el artículo 6 de la Ley de Acceso a la Información Pública, se entenderá por:

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando eso no requiera plazos o actividades desproporcionadas.

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 este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; identidad de los solicitantes de información, datos relativos a la

salud, a la vida, preferencia u orientación sexual, datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física.

Anonimización: La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re identificación de una persona sin esfuerzos desproporcionados.

Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, a fin de cumplir con el principio de transparencia.

Base de datos: es un conjunto de información de una persona, almacenada de forma estructurada y sistematizada, los cuales se pueden administrar, consultar, analizar y publicar. La base de datos puede estar alojada de manera local, bajo un servicio en la nube o un tercero (empresa privada o institución pública)

Consentimiento: Manifestación de voluntad, libre, inequívoca, informada y específica, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

Datos de acceso restringido: Aquellos datos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública.

Servicios en la nube: son los servicios que facilitan el procesamiento, almacenaje y disponibilidad de información, sistemas y herramientas las cuales se acceden por medio de Internet.

Deber de confidencialidad: Obligación de los responsables de bases de datos, personal a su cargo y del personal del Instituto de Acceso a la Información Pública, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la ley, principalmente cuando se acceda a información sobre datos personales.

Destinatario: Cualquier persona física o jurídica o privada que recibe datos personales.

Encargado: Prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de este.

Intermediario tecnológico o proveedor de servicios: Persona física o jurídica, pública o privada que brinda servicios en la nube, SaaS (software como un servicio), PaaS (Plataforma como un servicio), IaaS (Infraestructura como servicios) u otros servicios.

Estándares de seguridad: diferentes técnicas, controles y mecanismos que garantizan la seguridad para la administración, resguardo y eliminación de información, por ejemplo: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2 y SOC 3, PCI DSS.

Instituto: Instituto de Acceso a la Información Pública (IAIP).

LAIP: Ley de Acceso a la Información Pública.

LEPINA: Ley de Protección Integral de la Niñez y Adolescencia

LPA: Ley de Procedimientos Administrativos

NNA: Niños, Niñas y Adolescentes

Persona física identificable: Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

Responsable: Ente obligado que solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

Sistema de Registro: Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

Titular de los datos: Persona física o jurídica a quien le conciernen los datos personales.

Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y/o entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

Transmisor: Dependencia o entidad que posee los datos personales objeto de la transferencia.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizados sobre datos personales, relacionadas, de manera enunciativa más no limitativa con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Artículo 5.- Sistema de datos personales

Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

Físicos: Conjunto ordenado de datos personales que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

Automatizados: Conjunto ordenado de datos personales que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II Principios rectores de la Protección de los Datos Personales

Artículo 6.- Principios aplicables

En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Artículo 7.- Principio de Legitimación

Por regla general, el tratamiento de los datos personales únicamente podrá proceder en los siguientes supuestos:

1. Cuando el titular otorgue su consentimiento para una o varias finalidades específicas.
2. Sea necesario para el cumplimiento de una orden judicial, resolución u orden fundada y motivada por autoridad pública competente.
3. Sea necesario para el ejercicio de facultades propias de los entes obligados o se realice en virtud de una habilitación legal.
4. Sea necesario para el reconocimiento o defensa de los derechos del titular ante un ente obligado.
5. Sea necesario para la ejecución de un contrato o un precontrato en el que el titular sea parte.
6. Resulte necesario para proteger intereses vitales del titular o de otra persona física.
7. Sea necesario por razones de interés público establecidas o previstas por la Ley.

Artículo 8.- Principio de Licitud

El responsable tratará los documentos, sistemas o registros de datos personales, que estén en su poder, con estricto apego y cumplimiento de las atribuciones legales o reglamentarias de cada ente obligado y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe de ser determinada y legítima.

Artículo 9.- Principio de Lealtad

El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar estos a través de medios engañosos o fraudulentos.

Para estos efectos, se considerarán desleales aquellos tratamientos de datos personales que fueren contrarios al consentimiento brindado por el titular que den lugar a una discriminación injusta o arbitraria contra los titulares.

Artículo 10.- Principio de Transparencia

El responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

El responsable proporcionará al titular, al menos, la información siguiente:

- a. Su nombre y datos de contacto.
- b. Las finalidades del tratamiento a que serán sometidos sus datos personales.
- c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.
- d. La existencia, forma, mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación u oposición.
- e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

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.

El Instituto emitirá la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.

Artículo 11.- Principio de Finalidad

Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legitimadas por la ley o normativa administrativa pertinente.

El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

Artículo 12.- Principio de Proporcionalidad

El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

Artículo 13.- Principio de Calidad

El responsable adoptará las medidas pertinentes para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable por medio de la persona delegada para su tratamiento solicitará la supresión o eliminación de 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 irreversible y segura de la información.

Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifican su tratamiento o aquellas relacionadas con exigencias legales aplicables al responsable.

Artículo 14.- Principio de Responsabilidad

Los datos personales serán debidamente custodiados y los Responsables, Encargados y los titulares deberán garantizar el manejo cuidadoso en su tratamiento.

El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Lineamientos, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

- I. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
- II. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
- III. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.
- IV. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.
- V. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
- VI. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

El responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

Artículo 15.- Principio de Seguridad

El responsable establecerá y mantendrá con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

- a) El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
- b) El estado de la técnica.
- c) Los costos de aplicación
- d) La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.
- e) El alcance, contexto y las finalidades del tratamiento.
- f) Las transferencias internacionales de datos personales que se realicen o pretendan realizar.
- g) El número de titulares.
- h) Las posibles consecuencias que se derivarían de una vulneración para los titulares.
- i) Las vulneraciones previas ocurridas en el tratamiento de datos personales.

El responsable llevará 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.

Artículo 16.- Principio de Confidencialidad

El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

Capítulo III: Tratamiento de datos personales

Artículo 17.- Tratamiento exacto, adecuado, pertinente y no excesivo

A efecto de cumplir con el principio de calidad a que se refiere el artículo 13 de los presentes Lineamientos, se considera que el tratamiento de datos personales es:

- a. Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;
- b. Adecuado: Cuando se observan las medidas de seguridad aplicables;
- c. Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y
- d. No excesivo: Cuando la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Artículo 18.- Tratamiento de datos personales de niñas, niños y adolescentes

En el tratamiento de datos personales de niñas, niños y adolescentes, el responsable deberá privilegiar el interés superior de estos y la garantía de reserva, en los términos previstos en la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA) y la Convención sobre los Derechos del Niño, así como observar lo dispuesto en la LAIP.

Artículo 19.- Corrección de oficio

En caso de que los Responsables y Encargados detecten que hay datos personales inexactos o incompletos de conformidad al Art. 32 letra “d” de la LAIP, deberán de oficio actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Artículo 20.- Conservación de los datos

Los datos personales que hayan sido objeto de tratamiento y no contengan valor histórico, científico, estadístico o contable, deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los Lineamientos relacionados con la Gestión Documental y Archivos emitidos por este Instituto, teniendo en cuenta los siguientes plazos:

- a. El que se haya establecido en el formato físico o electrónico por el cual se recabaron;
- b. El establecido por las disposiciones aplicables;
- c. El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y
- d. El señalado en los casos de transferencia.

Artículo 21.- Condiciones técnicas

Los datos personales sólo podrán ser tratados en registros o sistemas de datos personales, tanto físicos como automatizados, que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Artículo 22.- Medios para recabar los datos

Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en los artículos 11, 15 y 16 de los presentes Lineamientos y 34 de la LAIP.

Artículo 23.- Disociación de datos

La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la normativa vigente y demás disposiciones aplicables.

Artículo 24.- Tratamiento de datos por el encargado

Cuando se contrate a un encargado para que realice el tratamiento de datos personales, deberá estipularse en el contrato respectivo las condiciones de utilización de los datos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, así como la determinación de responsabilidades por su incumplimiento.

Artículo 25.- Procedimientos para el tratamiento.

El responsable establecerá y documentará los procedimientos para la administración, resguardo, modificación, bloqueo y supresión de los datos personales. También, determinará los mecanismos administrativos, tecnológicos y físicos para garantizar la seguridad y el acceso no autorizado a los datos personales.

El responsable del tratamiento de los datos personales, debe cumplir los estándares mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales, sean estos resguardados de forma local, servicios en la nube o en servicios de instituciones públicas. Además, deberá velar por la aplicación del principio de calidad de la información.

Artículo 26.- Condiciones del tratamiento.

Corresponde al responsable o al encargado, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el titular, aún y cuando estos datos sean almacenados o alojados por un intermediario tecnológico.

Artículo 27.- Contratación o subcontratación de servicios.

Se podrá contratar o subcontratar los servicios de terceros, siempre y cuando estos cumplan con los estándares mínimos de seguridad en los servicios e infraestructura que ofrecen.

Artículo 28.- Tratamiento de datos por parte del encargado.

El encargado solo podrá intervenir en el tratamiento de las bases de datos personales, según lo establecido en el contrato celebrado con el responsable y sus indicaciones.

Para tal efecto, el encargado tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

- a. Tratar únicamente los datos personales conforme a las instrucciones del responsable;
- b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- c. Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, los presentes Lineamientos y las demás disposiciones aplicables;
- d. Guardar confidencialidad respecto de los datos personales tratados;
- e. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable.
- f. Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Capítulo IV: Derechos de los Titulares y su ejercicio

Del ejercicio de los derechos de acceso, rectificación, cancelación

Artículo 29.- Derechos ARCO

En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación y oposición de los datos personales que le conciernen.

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

Artículo 30.- Derecho de Acceso

De acuerdo con el Artículo 36 literales “a”, “b” y “c” de la LAIP, los titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, cualquier información relacionada a las condiciones generales y específicas de su tratamiento, lo siguiente:

- a. La información contenida en documentos o registros sobre su persona.
- b. Informe sobre finalidad para la que se ha recabado la información.
- c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control, en los términos del artículo 63 de la LAIP.

Artículo 31.- Alcances del Derecho de Acceso

El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:

- a. Obtener en intervalos razonables, según se dispone en la LAIP y en su caso en los plazos previstos en la Ley de Procedimientos Administrativos (LPA), sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.
- b. Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.
- c. Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.
- d. Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

Artículo 32.- Derecho de Rectificación

De conformidad al Artículo 36 literal “d” de la LAIP, los titulares de los datos personales tendrán el derecho a obtener de los entes obligados, la rectificación o corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.

Artículo 33.- Derecho de Cancelación

De conformidad al Artículo 36 literal “d” de la LAIP, los titulares tendrán derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, por falta de relevancia, actualidad de la información o por haberse cumplido el fin para el cual fueron recopilados; en razón de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 34.- Derecho de Oposición

De conformidad al Artículo 24 letra "b" y al Artículo 36 letra "d" de la LAIP, el titular podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular.

Artículo 35.- Personas facultadas para el ejercicio de los derechos ARCO

Los derechos ARCO conforme a lo establecido en los Arts. 31 y 36 de LAIP, serán ejercidos por su titular o su representante, quienes deberán acreditar su identidad al presentar su solicitud.

Artículo 36.- Ejercicio de los derechos ARCO a través de representante

Para el caso, el representante deberá adjuntar a su solicitud, Poder Especial en donde conste su acreditación, conforme a lo dispuesto en los Arts. 51 del Reglamento de la LAIP y 7 de los Lineamientos para la Recepción, Tramitación, Resolución y Notificación de solicitudes de acceso a la Información Pública.

Artículo 37.- Ejercicio de los derechos ARCO de las niñas, niños y adolescentes (NNA) y personas en situación de discapacidad.

Las niñas, niños y adolescentes "NNA" conforme a los Arts. 3 y 10 de la LEPINA, podrán acceder a su información personal por sí mismos o por medio de su madre, padre y otros representantes.

Los NNA menores de 14 años de edad, podrán ejercer los derechos de cancelación, rectificación y oposición a través de su madre, padre u otros representantes; en el caso de los mayores de 14 años de edad podrán ejercerlo directamente o a través de los antes mencionados, conforme lo dispuesto en los Arts. 10, 12 y 218 de la LEPINA.

En el caso, de las personas declaradas incapaces conforme a la ley, se estará a lo dispuesto en los Arts. 293 y 295 del Código Familia en lo que resulten aplicables.

Artículo 38.- Ejercicio de los derechos ARCO de personas fallecidas

Tratándose de datos personales concernientes a personas fallecidas, tendrán derecho a ejercerlos aquellos que acrediten un interés jurídico y podrán alegarse de manera enunciativa más no limitativa, los siguientes:

- a. Los parientes por consanguinidad en línea recta y en línea colateral hasta el cuarto grado de consanguinidad y en el de afinidad hasta el segundo, conforme a lo establecido en el Artículo 132 del Código de Familia.
- b. El albacea, legatario, heredero, asegurado siempre y cuando el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato legal y judicial para dicho efecto.

Por interés jurídico aquel que tiene una persona física que, con motivo del fallecimiento del titular, pretende ejercer los derechos ARCO de éste, para el reconocimiento de derechos sucesorios u otros similares.

Artículo 39.- Medios para la acreditación de la identidad del titular

El titular podrá acreditar su identidad a través de los siguientes medios:

- I. Documento Único de Identidad o pasaporte
- II. Otros documentos que permitan su identificación fehacientemente.

En el caso que el titular sea un NNA, su identidad se podrá acreditar mediante certificación de partida de nacimiento, credenciales expedidas por instituciones educativas y pasaporte. Si el titular es una persona en estado de incapacidad podrá acreditar su identidad por cualquiera de los documentos mencionados en este inciso; además de Documento Único de Identidad en el caso que lo posea.

Artículo 40.- Medios para la acreditación de la identidad y personalidad del representante

Cuando el titular ejerza sus derechos ARCO a través de su representante, este deberá acreditar la identidad del titular y su identidad y personalidad presentando ante el responsable lo siguiente:

- I. Identificación del representante
- II. Copia certificada de poder especial, en donde se le faculte específicamente para tal efecto.

Artículo 41.- Acreditación de los NNA cuando sus padres ejerzan la representación legal

En el caso que los padres de los NNA, pretendan ejercer los derechos ARCO de estos, además de acreditar la identidad de ellos en los términos descritos en el Art. 37 inciso segundo, se deberá acreditar la identidad y representación de los padres, con los siguientes documentos:

- I. Documento Único de Identidad o pasaporte, del padre que pretenda ejercer el derecho
- II. Documento legal o judicial que acredite el ejercicio de la representación legal

Artículo 42.- Acreditación de los NNA sujetos a tutela

Cuando el titular sea un NNA, además de acreditar la identidad de éste en los términos descritos en el Art. 37 inciso segundo, el tutor o representante legal deberá acreditar su identidad y representación con los siguientes documentos:

- I. Documento Único de Identidad del tutor.

- II. Documento legal o judicial que acredite la tutela

Artículo 43.- Acreditación del tutor o representante legal de una persona en estado de incapacidad

Cuando el titular sea una persona en estado de incapacidad y se le haya nombrado tutor o se haya decretado la prórroga o restablecimiento de la autoridad parental; además, de acreditar la identidad de este, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

- I. Documento Único de identidad del tutor o representante legal
- II. Documento legal o judicial que acredite la tutela, prórroga o restablecimiento de la autoridad parental.

Artículo 44.- Acreditación de las personas vinculadas a fallecidos

En los términos establecido en el Art. 38 de los presentes Lineamientos, la persona que pretenda ejercer los derechos ARCO de una persona fallecida, deberá presentar la siguiente documentación:

- I. Acta de defunción del titular
- II. Documento Único de Identidad de quien pretenda ejercer el derecho
- III. Documento y alegaciones que acrediten el interés jurídico que pretende ejercer.

Capítulo V: Tramitación de las solicitudes de datos personales

Artículo 45.- Solicitudes de acceso a datos personales

Para la tramitación de solicitudes de acceso información personal se estará a lo dispuesto en los artículos 36, 37, 66, 67, 68, 69, 70, 71, 72, 73 y 74 de la LAIP; al capítulo XI de su Reglamento y a lo establecido por este Instituto en el capítulo II de los Lineamientos para la recepción, tramitación, resolución y notificación de solicitudes de acceso a la información pública, en lo que fuera aplicable.

Artículo 46.- Documentos que deben acompañar las solicitudes de rectificación, cancelación y oposición de datos personales

Cuando el titular de los datos personales o su representante, solicite al oficial de información del ente obligado, la rectificación, cancelación u oposición de sus datos personales o en su caso los de su representado, deberán acompañar a su solicitud la documentación que respalde dicha petición; es decir, en donde conste la situación actual del dato personal, en virtud de la cual procedería una modificación, cancelación u oposición.

Artículo 47.- Plazos para la tramitación de solicitudes de acceso a datos personales

El Oficial de Información debe cumplir lo solicitado por el titular de los datos personales, tramitar de manera gratuita, y resolver en el sentido que corresponda en el plazo de diez días hábiles, contados a partir de la recepción de la solicitud o de la subsanación de la prevención, conforme a lo dispuesto en el Art. 66 de LAIP. En caso de la rectificación, actualización, confidencialidad o supresión de la información, el plazo será de treinta días hábiles desde la presentación de la solicitud de información.

En los casos de la ampliación de los plazos en materia de solicitudes de datos personales, solo aplica para el acceso a la información personal de conformidad con el Art. 71 de la LAIP, no así para las otras peticiones enmarcadas en el Art. 36 letra “d” de la ley. Asimismo, se contabiliza el nuevo plazo desde la fecha que se da la ampliación.

Artículo 48.- Tramitación y envío de información de carácter personal por medios electrónicos

Las solicitudes de datos personales podrán ser presentadas por medio de correo electrónico, debiendo enviar el formulario o escrito correspondiente en el que conste firma o huella junto con el documento que acredite la identidad del titular. Para el caso de los representantes, deben adjuntar los documentos que establecen estos Lineamientos, de manera escaneada u otro medio análogo.

En el caso, de la documentación que acredite la legitimación de los representantes, que ha sido remitida conforme al inciso anterior, deberá ser remitida de manera física al ente obligado veinticuatro horas después de haber sido enviada la solicitud, esta situación no afectará el cómputo de los plazos conforme al artículo anterior.

Capítulo VI

De la transferencia

Artículo 49.- Transferencia de los datos personales

Los entes obligados sólo podrán transferir datos personales cuando:

- a. Así lo prevea de manera expresa una disposición legal,
- b. Medie el consentimiento expreso de los titulares,
- c. Cuando se transmitan entre entes obligados, siempre y cuando exista una disposición legal o constitucional que lo habilite y se destinen al ejercicio específico de sus facultades.

El receptor de los datos transferidos podrá utilizarlos únicamente para los fines que motivaron la transferencia, salvo que se trate de fuentes de acceso público en general o se transfieran datos personales a organizaciones internacionales en cumplimiento a Tratados vigentes.

Artículo 50.- Deber de informar al Instituto

Los Oficiales de Información deberán rendir informe a este Instituto, en los términos establecidos en los presentes Lineamientos, sobre las transferencias totales o parciales de sistemas de datos personales que realice el ente obligado.

Artículo 51.- Requisitos del Informe

El informe a que hace referencia el artículo anterior deberá contener al menos, lo siguiente:

1. Identificación del Sistema de datos personales, del transferente y del destinatario de los datos;
2. Finalidad de la transferencia; así como el tipo de datos que son objeto de la transferencia;
3. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transferente y destinatario;
4. Plazo por el que conservará el destinatario los datos que le hayan sido transferidos, el cual podrá ser ampliado mediante aviso al Instituto, y
5. Señalar si una vez concluidos los propósitos de la transferencia, los datos personales deberán ser destruidos o devueltos al transferente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

Capítulo VII

De la Seguridad de los Sistemas de Datos Personales

Artículo 52.- Medidas de seguridad

Para proveer seguridad a los sistemas de datos personales, los titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

- a. Designar al área responsable de acuerdo a la normativa aplicable a cada ente, las cuales deben tener conocimiento sobre la materia;
- b. Proponer, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos, conforme al Art. 32 letra "e" de la LAIP;
- c. Proponer la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y
- d. Proponer la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a todo el personal y usuarios.

Lo dispuesto en el literal “b” debe ser remitido al Instituto para dar cumplimiento al Art. 35 de la LAIP.

Artículo 53.- Acciones sobre seguridad

En cada dependencia o entidad, se designará una Comisión o Comité interdisciplinario que coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales tanto físicos como electrónicos, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Artículo 54.- Reserva de la información

Los entes obligados conforme a lo establecido en el Art. 28 del Reglamento de la LAIP, podrán proponer la reserva de la documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica siempre y cuando coincida con alguna de las causales del Art. 19 y de los requisitos establecidos en el Art. 21 de la LAIP.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales, así como del contenido de éstos.

Artículo 55.- Resguardo de sistemas de datos personales físico y electrónico

El Responsable deberá:

- a. Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;
- b. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados, área responsable y usuarios titulares de los datos personales, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico,
- c. Informar al Comité los nombres de los Encargados y usuarios titulares de los datos personales.
- d. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;
- e. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales debiendo registrarse para ello en una bitácora;

- f. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en los presentes Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;
- g. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los Usuarios que utilizan datos personales, considerando al menos las siguientes actividades:
 - Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y
 - Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.
- h. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;
- i. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia; y
- j. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Artículo 56.- Seguridad en la red

En relación con los aspectos de seguridad, al utilizar la red de comunicación donde se transfieran datos personales, será obligatorio para los entes obligados establecer:

- a. Procedimientos de control de acceso a la red que consideren perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los Sistema de datos personales;
- b. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los sistemas de datos personales.

Artículo 57.- Documento de seguridad

Los entes obligados, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirá un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Artículo 58.- Requisitos mínimos del documento de seguridad

El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

- a. El nombre, cargo y adscripción de los Responsables, Encargados, Área Responsable y Usuarios;
- b. Estructura y descripción de los registros y sistemas de datos personales;
- c. Especificación detallada del tipo de datos personales contenidos en el sistema;
- d. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;
- e. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos,
- f. Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del sistema o registros de datos personales;
- g. Actualización de información contenida en el registro o sistema de datos personales;
- h. Procedimientos de creación de copias de respaldo y de recuperación de los datos;
- i. Bitácoras de acciones llevadas a cabo en el registro o sistema de datos personales;
- j. Procedimiento de notificación, gestión y respuesta ante incidentes; y
- k. Procedimiento para la cancelación del registro o sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Artículo 59.- Registro de incidentes

El área responsable deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Artículo 60.- Accesos controlados y bitácoras

En cada acceso a un registro o sistema de datos personales deberá guardarse como mínimo:

- a. Datos completos del Responsable, Encargado o Usuario;
- b. Modo de autenticación del Responsable, Encargado o Usuario;
- c. Fecha y hora en que se realizó el acceso, o se intentó el mismo;
- d. Registro o sistema de datos personales accedido;
- e. Operaciones o acciones llevadas a cabo dentro del registro o sistema de datos personales; y
- f. Fecha y hora en que se realizó la salida del registro o sistema de datos personales.

Artículo 61.-Operaciones de acceso, actualización, respaldo y recuperación

En las actividades relacionadas con la operación de los registros o sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:

- a. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, Encargados o Usuarios de los registros o sistemas de datos personales;
- b. Llevar control de los registros y sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transferencia de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad;
- c. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de datos personales;
- d. Mecanismos de auditoría o rastreabilidad de operaciones;
- e. Garantizar que el personal que trata datos personales, sólo tenga acceso a las funciones autorizadas de los registros o sistema de datos personales según su perfil de Usuario;
- f. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;

- g. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;
- h. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los registros o sistemas de datos personales;
- i. Garantizar que durante la transferencia de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;
- j. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;
- k. En los casos en que la operación sea externa, convenir con el encargado del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;
- l. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;
- m. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente respecto de medidas técnicas establecidas en los presentes Lineamientos y en su caso, remitirlos al Órgano Interno de Control, y;
- n. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el capítulo II de los presentes Lineamientos.

Estas medidas deberán ser integradas como anexos técnicos al documento de seguridad mencionado en el Artículo 38 de los presentes Lineamientos.

Capítulo VIII Registro del Sistema de datos personales

Artículo 63.-Datos del registro

Los registros o sistema de datos personales deberán contener, los siguientes datos:

- a. Nombre del registro o sistema;
- b. Unidad administrativa en la que se encuentra el registro o sistema;
- c. Nombre del área responsable del registro o sistema;
- d. Cargo del jefe del área responsable;

- e. Teléfono y correo electrónico del jefe del área responsable;
- f. Finalidad del registro o sistema, y
- g. Normatividad aplicable al registro o sistema.

El Instituto otorgará al Responsable un folio de identificación por cada Sistema de datos personales registrado.

Artículo 64.- Resolución de Inscripción

Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema “persona”, a efecto de dar cumplimiento a lo establecido en los Art. 35 de la LAIP.

Artículo 62.- Los Responsables deberán registrar e informar al Instituto, en un primer momento, dentro de los primeros diez días hábiles de enero y, una segunda vez, dentro de los primeros diez días hábiles de julio de cada año, lo siguiente:

- a. Los registros y sistemas de datos personales;
- b. Cualquier modificación sustancial o cancelación de dichos registros o sistemas, y;
- c. Cualquier transferencia de registros o sistemas de datos personales de conformidad a lo dispuesto en los presentes Lineamientos.

No obstante lo anterior, en caso de existir modificación sustancial en cualquiera de los supuestos anteriores, el Responsable deberá informar de manera inmediata al Instituto.

Capítulo VII

Del Instituto

Artículo 65.- Atribuciones

Son atribuciones del Instituto, además de las otras que le impongan la Ley u otras normas, las siguientes en materia de protección de datos personales:

- a. Velar por el cumplimiento de la normativa en materia de protección de datos.
- b. Llevar un registro que contenga una lista actualizada de los registros y sistemas de datos personales conforme al Art. 35 de la LAIP.
- b. Requerir al responsable los documentos mencionados en los presentes Lineamientos

- c. Acceder a los registros, sistemas o documentos de datos personales reguladas por los presentes Lineamientos, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante el Instituto, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.
- d. Resolver sobre las denuncias en materia de datos personales, conforme a las infracciones establecidas en el Art. 76 de la LAIP; además de los artículos 71 y 150 de la LPA.
- e. Ordenar de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de la información contenida en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales.
- f. Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
- g. Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
- h. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.
- i. Emitir la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.
- j. Formar y capacitar, a través de la Unidad de Capacitaciones y Formación de este Instituto, sobre materia de protección de datos personales.

En el ejercicio de sus atribuciones, el Instituto deberá emplear procedimientos automatizados de acuerdo con las mejores herramientas tecnológicas a su alcance.

Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los registros o sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la ley, su reglamento, los presentes Lineamientos y las demás leyes relacionadas al tema.

Capítulo VII

Disposiciones transitorias

Artículo 66.- Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los Titulares de los mismos; es decir, sobre la finalidad de los registros o sistema de datos personales, deberán ser elaborados en términos de los presentes Lineamientos y deberán comenzar a utilizarse, a más tardar en un plazo de un año a partir de la vigencia de los presentes Lineamientos.

Artículo 67.- En tanto y a más tardar dentro de un mes, siguiente a la entrada en vigor de los presentes Lineamientos, las dependencias y entidades que recaben datos personales deberán informar a los Titulares de los mismos, un documento por separado en el que se detalle los propósitos para los cuales éstos se recaban.

Artículo 68.- El cumplimiento de las disposiciones contenidas en los presentes Lineamientos deberá efectuarse a más tardar en un plazo de seis meses posterior a su entrada en vigor.

En el caso del documento de seguridad y registros o sistemas de bases de datos a la cual se refiere el Lineamiento en los capítulos VII y VIII, su cumplimiento deberá efectuarse en un plazo de un año posterior a su entrada en vigor.

Artículo 69.- El Instituto deberá efectuar las siguientes acciones:

- a. Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes Lineamientos y el manual de protección de datos, en un plazo máximo de tres meses a partir de la publicación de este último.
- b. Elaborar las recomendaciones sobre las medidas de seguridad que se mencionan en los presentes Lineamientos, a más tardar en un plazo de tres meses a partir de su entrada en vigor.

Capítulo VIII

Disposiciones finales

Artículo 70.- Los presentes Lineamientos entrarán en vigor seis meses después de su publicación en el Diario Oficial.

Artículo 71.- Así lo acordaron por unanimidad los Comisionados del Instituto de Acceso a la Información Pública.-

Correlativo	Sección	Total de comentarios activos	Total de comentarios inactivos	Total de votos a favor	Total de votos en contra
1	LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES				
2	Considerando				
3	<p>I. Que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;</p>			3	
4	<p>II. Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;</p>	3		1	
5	<p>III. Que los avances tecnológicos y el progreso de la sociedad de la información ofrecen a los individuos herramientas que contribuyen a mejorar su calidad de vida. Asimismo, coadyuvan con el Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste. Por otra parte, las nuevas tecnologías facilitan ilimitadas posibilidades para transmitir un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;</p>				

2

11	IX. Que la Ley de Acceso a la Información Pública es obligatoria para los poderes públicos de la República de El Salvador, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;				
12	X. Que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica el tratamiento de datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, responsabilidad, de información al titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transferencia;				
13	XI. Que es de gran relevancia que las personas tengan conocimiento de la información que de ellos obra en los archivos del Sector Público a efecto de hacer uso de los derechos de acceso, rectificación, cancelación y oposición de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman;				
14	XII. Que el Instituto de Acceso a la Información Pública es el garante de la protección de la información de carácter personal, a efecto de evitar injerencias a su vida privada, en equilibrio con los principios de Transparencia y Acceso a la Información Pública Gubernamental que se requieren para un desarrollo del Estado Democrático de Derecho;				
15	Capítulo I: Disposiciones generales				

[illegible]

27	Se reconoce el derecho de toda persona a la protección de datos personales, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.				
28	Artículo 4.- Definiciones				
29	Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en el artículo 6 de la Ley de Acceso a la Información Pública, se entenderá por:				
30	Datos Personales: Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando eso no requiera plazos o actividades desproporcionadas.			1	
31	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 este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; identidad de los solicitantes de información, datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física.				
32	Anonimización: La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re identificación de una persona sin esfuerzos desproporcionados.				
33	Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, a fin de cumplir con el principio de transparencia.				
34	Base de datos: es un conjunto de información de una persona, almacenada de forma estructurada y sistematizada, los cuales se pueden administrar, consultar, analizar y publicar. La base de datos puede estar alojada de manera local, bajo un servicio en la nube o un tercero (empresa privada o institución pública)				

35	Consentimiento: Manifestación de voluntad, libre, inequívoca, informada y específica, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.				
36	Datos de acceso restringido: Aquellos datos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública.				
37	Servicios en la nube: son los servicios que facilitan el procesamiento, almacenaje y disponibilidad de información, sistemas y herramientas las cuales se acceden por medio de Internet.				
38	Deber de confidencialidad: Obligación de los responsables de bases de datos, personal a su cargo y del personal del Instituto de Acceso a la Información Pública, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la ley, principalmente cuando se acceda a información sobre datos personales.				
39	Destinatario: Cualquier persona física o jurídica o privada que recibe datos personales.				
40	Encargado: Prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de este.				
41	Intermediario tecnológico o proveedor de servicios: Persona física o jurídica, pública o privada que brinda servicios en la nube, SaaS (software como un servicio), PaaS (Plataforma como un servicio), IaaS (Infraestructura como servicios) u otros servicios.				
42	Estándares de seguridad: diferentes técnicas, controles y mecanismos que garantizan la seguridad para la administración, resguardo y eliminación de información, por ejemplo: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2 y SOC 3, PCI DSS.				
43	 Instituto: Instituto de Acceso a la Información Pública (IAIP).				
44	LAIP: Ley de Acceso a la Información Pública.				
45	LEPINA: Ley de Protección Integral de la Niñez y Adolescencia				
46	LPA: Ley de Procedimientos Administrativos				
47	NNA: Niños, Niñas y Adolescentes				

48	Persona física identificable: Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.				
49	Responsable: Ente obligado que solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.				
50	Sistema de Registro: Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.				
51	Titular de los datos: Persona física o jurídica a quien le conciernen los datos personales.				
52	Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y/o entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.				
53	Transmisor: Dependencia o entidad que posee los datos personales objeto de la transferencia.				
54	Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizados sobre datos personales, relacionadas, de manera enunciativa más no limitativa con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.				
55	Artículo 5.- Sistema de datos personales				
56	Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.				

[illegible]

[illegible]

10

93	Artículo 12.- Principio de Proporcionalidad				
94	El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.				
95	Artículo 13.- Principio de Calidad				
96	El responsable adoptará las medidas pertinentes para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.				
97	Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable por medio de la persona delegada para su tratamiento solicitará la supresión o eliminación de archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.				
98	En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación irreversible y segura de la información.				
99	Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifican su tratamiento o aquellas relacionadas con exigencias legales aplicables al responsable.				
100	Artículo 14.- Principio de Responsabilidad				
101	Los datos personales serán debidamente custodiados y los Responsables, Encargados y los titulares deberán garantizar el manejo cuidadoso en su tratamiento.				

102	El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Lineamientos, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.				
103	Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.				
104	Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:				
105	I. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.				
106	II. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.				
107	III. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.				
108	IV. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.				

13

119	d) La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.				
120	e) El alcance, contexto y las finalidades del tratamiento.				
121	f) Las transferencias internacionales de datos personales que se realicen o pretendan realizar.				
122	g) El número de titulares.				
123	h) Las posibles consecuencias que se derivarían de una vulneración para los titulares.				
124	i) Las vulneraciones previas ocurridas en el tratamiento de datos personales.				
125	El responsable llevará 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.				
126	Artículo 16.- Principio de Confidencialidad				
127	El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.				
128	Capítulo III: Tratamiento de datos personales				
129	Artículo 17.- Tratamiento exacto, adecuado, pertinente y no excesivo				
130	A efecto de cumplir con el principio de calidad a que se refiere el artículo 13 de los presentes Lineamientos, se considera que el tratamiento de datos personales es:				

[illegible]

16

150	La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.				
151	El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la normativa vigente y demás disposiciones aplicables.				
152	Artículo 24.- Tratamiento de datos por el encargado				
153	Cuando se contrate a un encargado para que realice el tratamiento de datos personales, deberá estipularse en el contrato respectivo las condiciones de utilización de los datos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, así como la determinación de responsabilidades por su incumplimiento.				
154	Artículo 25.- Procedimientos para el tratamiento.				
155	El responsable establecerá y documentará los procedimientos para la administración, resguardo, modificación, bloqueo y supresión de los datos personales. También, determinará los mecanismos administrativos, tecnológicos y físicos para garantizar la seguridad y el acceso no autorizado a los datos personales.				
156	El responsable del tratamiento de los datos personales, debe cumplir los estándares mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales, sean estos resguardados de forma local, servicios en la nube o en servicios de instituciones públicas. Además, deberá velar por la aplicación del principio de calidad de la información.				
157	Artículo 26.- Condiciones del tratamiento.				
158	Corresponde al responsable o al encargado, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el titular, aún y cuando estos datos sean almacenados o alojados por un intermediario tecnológico.				

18

172	Artículo 29.- Derechos ARCO				
173	En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación y oposición de los datos personales que le conciernen.				
174	El ejercicio de cualquiera de los derechos referidos no es requisito previo, ni impide el ejercicio de otro.				
175	Artículo 30.- Derecho de Acceso				
176	De acuerdo con el Artículo 36 literales "a", "b" y "c" de la LAIP, los titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, cualquier información relacionada a las condiciones generales y específicas de su tratamiento, lo siguiente:				
177	a. La información contenida en documentos o registros sobre su persona.				
178	b. Informe sobre finalidad para la que se ha recabado la información.				
179	c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control, en los términos del artículo 63 de la LAIP.				
180	Artículo 31.- Alcances del Derecho de Acceso				
181	El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:				
182	a. Obtener en intervalos razonables, según se dispone en la LAIP y en su caso en los plazos previstos en la Ley de Procedimientos Administrativos (LPA), sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.				

183	b. Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.				
184	c. Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.				
185	d. Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.				
186	Artículo 32.- Derecho de Rectificación				
187	De conformidad al Artículo 36 literal "d" de la LAIP, los titulares de los datos personales tendrán el derecho a obtener de los entes obligados, la rectificación o corrección de sus datos personales, cuando estos resulten inexectos, incompletos o no se encuentren actualizados.				
188	Artículo 33.- Derecho de Cancelación				
189	De conformidad al Artículo 36 literal "d" de la LAIP, los titulares tendrán derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, por falta de relevancia, actualidad de la información o por haberse cumplido el fin para el cual fueron recopilados; en razón de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.				
190	Artículo 34.- Derecho de Oposición				
191	De conformidad al Artículo 24 letra "b" y al Artículo 36 letra "d" de la LAIP, el titular podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular.				

192	Artículo 35.- Personas facultadas para el ejercicio de los derechos ARCO				
193	Los derechos ARCO conforme a lo establecido en los Arts. 31 y 36 de LAIP, serán ejercidos por su titular o su representante, quienes deberán acreditar su identidad al presentar su solicitud.				
194	Artículo 36.- Ejercicio de los derechos ARCO a través de representante				
195	Para el caso, el representante deberá adjuntar a su solicitud, Poder Especial en donde conste su acreditación, conforme a lo dispuesto en los Arts. 51 del Reglamento de la LAIP y 7 de los Lineamientos para la Recepción, Tramitación, Resolución y Notificación de solicitudes de acceso a la Información Pública.				
196	Artículo 37.- Ejercicio de los derechos ARCO de las niñas, niños y adolescentes (NNA) y personas en situación de discapacidad.				
197	Las niñas, niños y adolescentes "NNA" conforme a los Arts. 3 y 10 de la LEPINA, podrán acceder a su información personal por sí mismos o por medio de su madre, padre y otros representantes.				
198	Los NNA menores de 14 años de edad, podrán ejercer los derechos de cancelación, rectificación y oposición a través de su madre, padre u otros representantes; en el caso de los mayores de 14 años de edad podrán ejercerlo directamente o a través de los antes mencionados, conforme lo dispuesto en los Arts. 10, 12 y 218 de la LEPINA.				
199	En el caso, de las personas declaradas incapaces conforme a la ley, se estará a lo dispuesto en los Arts. 293 y 295 del Código Familia en lo que resulten aplicables.				
200	Artículo 38.- Ejercicio de los derechos ARCO de personas fallecidas				
201	Tratándose de datos personales concernientes a personas fallecidas, tendrán derecho a ejercerlos aquellos que acrediten un interés jurídico y podrán alegarse de manera enunciativa más no limitativa, los siguientes:				

22

23

227	En los términos establecido en el Art. 38 de los presentes Lineamientos, la persona que pretenda ejercer los derechos ARCO de una persona fallecida, deberá presentar la siguiente documentación:				
228	I. Acta de defunción del titular				
229	II. Documento Único de Identidad de quien pretenda ejercer el derecho				
230	III. Documento y alegaciones que acrediten el interés jurídico que pretende ejercer.				
231	Capítulo V: Tramitación de las solicitudes de datos personales				
232	Artículo 45.- Solicitudes de acceso a datos personales				
233	Para la tramitación de solicitudes de acceso información personal se estará a lo dispuesto en los artículos 36, 37, 66, 67, 68, 69, 70, 71, 72, 73 y 74 de la LAIP; al capítulo XI de su Reglamento y a lo establecido por este Instituto en el capítulo II de los Lineamientos para la recepción, tramitación, resolución y notificación de solicitudes de acceso a la información pública, en lo que fuera aplicable.				
234	Artículo 46.- Documentos que deben acompañar las solicitudes de rectificación, cancelación y oposición de datos personales				
235	Cuando el titular de los datos personales o su representante, solicite al oficial de información del ente obligado, la rectificación, cancelación u oposición de sus datos personales o en su caso los de su representado, deberán acompañar a su solicitud la documentación que respalde dicha petición; es decir, en donde conste la situación actual del dato personal, en virtud de la cual procedería una modificación, cancelación u oposición.				
236	Artículo 47.- Plazos para la tramitación de solicitudes de acceso a datos personales				

237	El Oficial de Información debe cumplir lo solicitado por el titular de los datos personales, tramitar de manera gratuita, y resolver en el sentido que corresponda en el plazo de diez días hábiles, contados a partir de la recepción de la solicitud o de la subsanación de la prevención, conforme a lo dispuesto en el Art. 66 de LAIP. En caso de la rectificación, actualización, confidencialidad o supresión de la información, el plazo será de treinta días hábiles desde la presentación de la solicitud de información.				
238	En los casos de la ampliación de los plazos en materia de solicitudes de datos personales, solo aplica para el acceso a la información personal de conformidad con el Art. 71 de la LAIP, no así para las otras peticiones enmarcadas en el Art. 36 letra "d" de la ley. Asimismo, se contabiliza el nuevo plazo desde la fecha que se da la ampliación.				
239	Artículo 48.- Tramitación y envío de información de carácter personal por medios electrónicos				
240	Las solicitudes de datos personales podrán ser presentadas por medio de correo electrónico, debiendo enviar el formulario o escrito correspondiente en el que conste firma o huella junto con el documento que acredite la identidad del titular. Para el caso de los representantes, deben adjuntar los documentos que establecen estos Lineamientos, de manera escaneada u otro medio análogo.				
241	En el caso, de la documentación que acredite la legitimación de los representantes, que ha sido remitida conforme al inciso anterior, deberá ser remitida de manera física al ente obligado veinticuatro horas después de haber sido enviada la solicitud, esta situación no afectará el cómputo de los plazos conforme al artículo anterior.				
242	Capítulo VI				
243	De la transferencia				
244	Artículo 49.- Transferencia de los datos personales				
245	Los entes obligados sólo podrán transferir datos personales cuando:				
246	a. Así lo prevea de manera expresa una disposición legal,				

247	b. Medie el consentimiento expreso de los titulares,				
248	c. Cuando se transmitan entre entes obligados, siempre y cuando exista una disposición legal o constitucional que lo habilite y se destinen al ejercicio específico de sus facultades.				
249	El receptor de los datos transferidos podrá utilizarlos únicamente para los fines que motivaron la transferencia, salvo que se trate de fuentes de acceso público en general o se transfieran datos personales a organizaciones internacionales en cumplimiento a Tratados vigentes.				
250	Artículo 50.- Deber de informar al Instituto				
251	Los Oficiales de Información deberán rendir informe a este Instituto, en los términos establecidos en los presentes Lineamientos, sobre las transferencias totales o parciales de sistemas de datos personales que realice el ente obligado.				
252	Artículo 51.- Requisitos del Informe				
253	El informe a que hace referencia el artículo anterior deberá contener al menos, lo siguiente:				
254	1. Identificación del Sistema de datos personales, del transferente y del destinatario de los datos;				
255	2. Finalidad de la transferencia; así como el tipo de datos que son objeto de la transferencia;				
256	3. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transferente y destinatario;				
257	4. Plazo por el que conservará el destinatario los datos que le hayan sido transferidos, el cual podrá ser ampliado mediante aviso al Instituto, y				

258	5. Señalar si una vez concluidos los propósitos de la transferencia, los datos personales deberán ser destruidos o devueltos al transferente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.				
259	Capítulo VII				
260	De la Seguridad de los Sistemas de Datos Personales				
261	Artículo 52.- Medidas de seguridad			1	
262	Para proveer seguridad a los sistemas de datos personales, los titulares de las dependencias y entidades deberán adoptar las medidas siguientes:			1	
263	a. Designar al área responsable de acuerdo a la normativa aplicable a cada ente, las cuales deben tener conocimiento sobre la materia;				
264	b. Proponer, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos, conforme al Art. 32 letra "e" de la LAIP;				
265	c. Proponer la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y				
266	d. Proponer la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a todo el personal y usuarios.				
267	Lo dispuesto en el literal "b" debe ser remitido al Instituto para dar cumplimiento al Art. 35 de la LAIP.				
268	Artículo 53.- Acciones sobre seguridad				

[illegible]

[illegible]

[illegible]

31

310	Artículo 60.- Accesos controlados y bitácoras				
311	En cada acceso a un registro o sistema de datos personales deberá guardarse como mínimo:				
312	a. Datos completos del Responsable, Encargado o Usuario;				
313	b. Modo de autenticación del Responsable, Encargado o Usuario;				
314	c. Fecha y hora en que se realizó el acceso, o se intentó el mismo;				
315	d. Registro o sistema de datos personales accedido;				
316	e. Operaciones o acciones llevadas a cabo dentro del registro o sistema de datos personales; y				
317	f. Fecha y hora en que se realizó la salida del registro o sistema de datos personales.				
318	Artículo 61.-Operaciones de acceso, actualización, respaldo y recuperación				
319	En las actividades relacionadas con la operación de los registros o sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:				
320	a. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, Encargados o Usuarios de los registros o sistemas de datos personales;				
321	b. Llevar control de los registros y sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transferencia de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad;				
322	c. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de datos personales;				

[illegible]

34

	Artículo 62.- Los				
348	Responsables deberán registrar e informar al Instituto, en un primer momento, dentro de los primeros diez días hábiles de enero y, una segunda vez, dentro de los primeros diez días hábiles de julio de cada año, lo siguiente:				
349	a. Los registros y sistemas de datos personales;				
350	b. Cualquier modificación sustancial o cancelación de dichos registros o sistemas, y;				
351	c. Cualquier transferencia de registros o sistemas de datos personales de conformidad a lo dispuesto en los presentes Lineamientos.				
352	No obstante lo anterior,				
	en caso de existir modificación sustancial en cualquiera de los supuestos anteriores, el Responsable deberá informar de manera inmediata al Instituto.				
353	Capítulo VII				
354	Del Instituto				
355	Artículo 65.- Atribuciones				
356	Son atribuciones del Instituto, además de las otras que le impongan la Ley u otras normas, las siguientes en materia de protección de datos personales: a. Velar por el cumplimiento de la normativa en materia de protección de datos.				
357	b. Llevar un registro que contenga una lista actualizada de los registros y sistemas de datos personales conforme al Art. 35 de la LAIP.				
358	b. Requerir al responsable los documentos mencionados en los presentes Lineamientos				
359	c. Acceder a los registros, sistemas o documentos de datos personales reguladas por los presentes Lineamientos, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante el Instituto, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.				
360					

[illegible]

369	Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los registros o sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la ley, su reglamento, los presentes Lineamientos y las demás leyes relacionadas al tema.				
370	Capítulo VII				
371	Disposiciones transitorias				
372	Artículo 66.- Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los Titulares de los mismos; es decir, sobre la finalidad de los registros o sistema de datos personales, deberán ser elaborados en términos de los presentes Lineamientos y deberán comenzar a utilizarse, a más tardar en un plazo de un año a partir de la vigencia de los presentes Lineamientos.				
373	Artículo 67.- En tanto y a más tardar dentro de un mes, siguiente a la entrada en vigor de los presentes Lineamientos, las dependencias y entidades que recaben datos personales deberán informar a los Titulares de los mismos, un documento por separado en el que se detalle los propósitos para los cuales éstos se recaban.				
374	Artículo 68.- El cumplimiento de las disposiciones contenidas en los presentes Lineamientos deberá efectuarse a más tardar en un plazo de seis meses posterior a su entrada en vigor.				
375	En el caso del documento de seguridad y registros o sistemas de bases de datos a la cual se refiere el Lineamiento en los capítulos VII y VIII, su cumplimiento deberá efectuarse en un plazo de un año posterior a su entrada en vigor.				
376	Artículo 69.- El Instituto deberá efectuar las siguientes acciones:				
377	a. Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes Lineamientos y el manual de protección de datos, en un plazo máximo de tres meses a partir de la publicación de este último.				

38



Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

Fwd: seguimiento a lineamientos publicados en LEGISLA para consulta pública

1 mensaje

Vicente Hernandez <vhernandez@iaip.gob.sv>

28 de enero de 2021, 23:58

Para: Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

----- Forwarded message -----

De: **Jorge Martínez** <jemartinez@iaip.gob.sv>

Date: mar, 31 mar 2020 a las 10:21

Subject: seguimiento a lineamientos publicados en LEGISLA para consulta pública

To: Johanna Clará <jduenas@iaip.gob.sv>, Rene Valiente <rvaliente@iaip.gob.sv>

Cc: Vicente Hernandez <vhernandez@iaip.gob.sv>

Buen día, espero se encuentren bien!

Les quiero recordar que es necesario brindar respuesta y justificación técnica a los procesos de consulta pública. En ese sentido, estoy a la espera de sus respuestas con base a los documentos que les he compartido con los comentarios recibidos.

Quedo a la espera de sus comentarios.

Saludos cordiales,




Jorge Martínez**Jefe de la Unidad de Tecnologías de la Información**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,

edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: jemartinez@iaip.gob.sv




Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*--
Vicente Hernandez**Oficial de Información**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,

edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: vhernandez@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*



Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

Fwd: Respuesta a las consultas realizadas a los lineamientos de PDP

1 mensaje

Vicente Hernandez <vhernandez@iaip.gob.sv>

28 de enero de 2021, 23:53

Para: Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

----- Forwarded message -----

De: **Johanna Clará** <jduenas@iaip.gob.sv>

Date: mié, 1 abr 2020 a las 16:03

Subject: Respuesta a las consultas realizadas a los lineamientos de PDP

To: Jorge Martínez <jemartinez@iaip.gob.sv>, Vicente Hernandez <vhernandez@iaip.gob.sv>

Buenas tardes, les remito el documento en el que se encuentran las respuestas a las observaciones realizadas a los lineamientos generales para la protección de datos personales para el sector público.




Cordialmente

Johanna Clará**Jefa de la Unidad de Protección de Datos Personales**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.




Correo Electrónico: jduenas@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"***Vicente Hernandez****Oficial de Información**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: vhernandez@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"***Lineamientos de datos personales, respuesta tecnica.xlsx**

71K

Fecha de comentario	Usuario	Sección	Comentario	Justificación técnica
12/3/2020	María	Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;	La protección de datos personales además de plantearse para los entes públicos, teniendo en cuenta que es un derecho humano, también debe plantearse para regular las acciones de los entes privados	El IAIP actualmente, de conformidad a la Ley de Acceso a la Información Pública, únicamente tiene la competencia para conocer respecto de la protección de datos personales (ello comprende el cumplimiento de los derechos ARCO: Acceso, Rectificación, Cancelación y Oposición) en poder de instituciones públicas y concesionarios de estas. Sin embargo, actualmente en la Comisión de Economía de la Asamblea Legislativa se encuentra en estudio la elaboración de la Ley de Protección de Datos Personales en el que ya se incluye tanto a los entes públicos como privados
5/3/2020	Laura Nathalie	Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;	Información de una persona física identificada, o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados, fundamentalmente en atención al empleo de tecnologías de la información y la comunicación.	La definición de datos personales brindada es muy acertada. El derecho a la protección de datos personales o a la autodeterminación informativa presupone la capacidad de las personas para decidir y controlar las actividades relacionadas con sus datos personales ante su posible uso indiscriminado, arbitrario o sin certeza sobre sus fines y límites. (sentencia del 4-III-2011, Amp. 934-2007; sentencia del 12-V-2017, Inc. 35-2016)
5/3/2020	Nelly Yohana Cuellar Rivera	Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;	datos personales: Información que le concierne e identifica...	Los datos personales, de acuerdo al artículo 6 letra a) de la Ley de Acceso a la Información Pública suponen la información privada concerniente a una persona, identificada o identificable; es decir, los datos personales suponen toda aquella información que es de dominio exclusivo de su titular y que, a su vez, permite identificarle con distinción de cualquier otra persona natural.



La infrascrita Directora Ejecutiva del Instituto de Acceso a la Información Pública hace constar que en el acta número doce de sesión ordinaria de fecha treinta de marzo de dos mil veinte, se acordó, en el punto siete, lo que se transcribe a continuación: **"PUNTO SIETE: Aprobación de los Lineamientos Generales de Protección de Datos Personales para Instituciones del Sector Público: El día 28 de febrero de 2020 los Lineamientos se subieron a la sitio web Legisla para someterlos a consulta pública, el plazo finalizó el 20 de marzo de 2020, teniendo únicamente 3 observaciones, las cuales, en lo posible, han sido incorporadas al documento final que conforman los lineamientos. Por lo que, se presenta a pleno para su respectiva aprobación y posterior publicación en el Diario Oficial. Se hace la aclaración que se incorporará una cláusula derogatoria de los lineamientos previos elaborados por el IAIP pero no publicados en el Diario Oficial porque tenían elementos que no estaban acorde a la realidad del país (eran más con respecto a la realidad de Costa Rica). Este documento, además, fue revisado profundamente en una sesión de trabajo previa. Al respecto, el punto no fue aprobado, existiendo un voto a favor, por parte de la Comisionada Silvia Pérez; y cuatro votos en contra, de las Comisionadas Liduvina Escobar, Daniela Huevo y Cesia Mena y el Comisionado Andrés Rodríguez, debido a que solicitaron que el documento sea enviado a la Unidad de Género para que se le incorpore lenguaje inclusivo en el lineamiento, sin alterar el fondo del articulado y aprobar con posterioridad el lineamiento en una sesión extraordinaria. Se instruye a la Directora Ejecutiva notificar este acuerdo a la Jefa de la Unidad de Género, solicitándole que revise los documentos a más tardar en la mañana del 1º de abril de 2020. El punto será retomado en sesión extraordinaria".** Extiende la presente en San Salvador, a un día del mes de febrero de dos mil veintiuno.

Licda. Miriam Marlene Chávez Alfaro
Directora Ejecutiva



59



Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

Fwd: Solicitud: revisión de lineamientos desde la U. de Género

Rocio Montes <rmontes@iaip.gob.sv>

29 de enero de 2021, 0:10

Para: Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

----- Forwarded message -----

De: **Rene Valiente** <rvaliente@iaip.gob.sv>

Date: jue, 2 abr 2020 a las 11:28

Subject: Re: Solicitud: revisión de lineamientos desde la U. de Género

To: Rocio Montes <rmontes@iaip.gob.sv>

Cc: Carlos Calderon <ccalderon@iaip.gob.sv>, Johanna Clará <jduenas@iaip.gob.sv>

muy agradecido Rocío.

El mié., 1 abr. 2020 a las 1:47, Rocio Montes (<rmontes@iaip.gob.sv>) escribió:

Buen día,

Adjunto las modificaciones con control de cambios, a efecto de determinar que no existen alteraciones de contenido de las disposiciones; sino únicamente modificaciones en cuanto al uso de lenguaje inclusivo, no sexista.

Saludos,

El lun., 30 mar. 2020 a las 12:32, Rene Valiente (<rvaliente@iaip.gob.sv>) escribió:

Comparto la versión final del Lineamiento para la Gestión de SOLICITUDES de Acceso a la Información Pública, para los efectos de incorporación de lenguaje inclusivo.

Saludos

El lun., 30 mar. 2020 a las 12:28, Carlos Calderon (<ccalderon@iaip.gob.sv>) escribió:


Carlos Calderon**Gerente de de la Unidad de Garantía y Protección de Derechos**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,

edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: ccalderon@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*

----- Forwarded message -----

De: **Miriam Chávez** <mchavez@iaip.gob.sv>

Date: lun., 30 mar. 2020 a las 12:18

Subject: Fwd: Solicitud: revisión de lineamientos desde la U. de Género




To: Carlos Calderon <ccalderon@iaip.gob.sv>

Miriam Chávez**Directora Ejecutiva**

Tel.:(503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: mchavez@iaip.gob.sv

Visítanos en:   



Instituto de Acceso
a la Información Pública



"Cuidemos el medio ambiente, imprima este correo solo si es necesario"

----- Forwarded message -----

De: **Miriam Chávez** <mchavez@iaip.gob.sv>

Date: lun., 30 de mar. de 2020 a la(s) 12:16

Subject: Solicitud: revisión de lineamientos desde la U. de Género

To: Rocio Montes <rmontes@iaip.gob.sv>

Cc: Cristy Cristina Pérez <sperez@iaip.gob.sv>

Hola, Rocío, buenas tardes.

En sesión de Pleno del día de hoy se acordó que los lineamientos de gestión de solicitudes de información y de protección de datos personales sean revisados por vos, para que, por favor, incorpores lenguaje inclusivo sin tocar el fondo de cada artículo.

Comentarte que esto debe de estar listo a más tardar el miércoles, 1 de abril por la mañana.

Además, se te solicita crear un lineamiento y una capacitación dirigida a las unidades que más documentos sacan para que puedan incorporar el lenguaje de género de una vez cuando creen la información.

Cordiales saludos.




Miriam Chávez

Directora Ejecutiva

Tel.:(503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: mchavez@iaip.gob.sv

Visítanos en:   



Instituto de Acceso
a la Información Pública



"Cuidemos el medio ambiente, imprima este correo solo si es necesario"

--

Rene Valiente

Jefe de la Unidad de Derecho de Acceso a la Información Pública

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: rvaliente@iaip.gob.sv

Visítanos en:   



Instituto de Acceso
a la Información Pública

"Cuidemos el medio ambiente, imprima este correo solo si es necesario"



60

--

Rocio Montes**Encargada Institucional de Género**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: rmontes@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*




--

Rene Valiente**Jefe de la Unidad de Derecho de Acceso a la Información Pública**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: rvaliente@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*




--

Rocio Montes**Encargada Institucional de Género**

Tel.:(503)2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: rmontes@iaip.gob.sv

Visítanos en:   Instituto de Acceso
a la Información Pública*"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*

El Pleno del INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA, en ejercicio de las atribuciones legales establecidas en los artículos 3 letras “a”, “b”, “e” y “g”; 10; 18 y 58 letra “j” de la Ley de Acceso a la Información Pública (LAIP) y **considerando:**

I. Que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;

LINEAMIENTOS GENERALES DE PROTECCION DE DATOS PERSONALES PARA INSTITUCIONES DEL SECTOR PÚBLICO

II. Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física identificada o identificable con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;

III. Que los avances tecnológicos y el progreso de la sociedad de la información ofrecen a ~~los individuos~~ las personas herramientas que contribuyen a mejorar su calidad de vida. Asimismo, coadyuvan con el Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste. Por otra parte, las nuevas tecnologías facilitan ilimitadas posibilidades para transmitir un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;

IV. Que, sin embargo, un tratamiento inadecuado de esas herramientas tecnológicas y de la información personal de ~~los habitantes~~ la población puede atentar contra la privacidad, seguridad y autodeterminación informativa de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo;

V. Que se requiere un nivel uniforme y elevado de protección de las personas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras injustificadas a sus derechos y acciones desproporcionadas con el uso de sus datos personales;

VI. Que, en el tratamiento de los datos personales, es imperioso establecer un equilibrio entre los intereses de ~~todos los actores~~ toda persona: del sector público, social y titulares ~~involucrados~~, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que sean acordes con los fines perseguidos en sociedades democráticas;

VII. Observando que el artículo 6 de la Constitución establece como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el orden público, la moral, el honor, y la vida privada;

VIII. Que a su vez el acceso a la información pública está consagrado como derecho fundamental que el Estado está llamado a proteger. En este sentido, las instituciones públicas cumplen un papel fundamental en la promoción de la transparencia en su gestión, siendo ~~los funcionarios~~ el funcionariado públicos depositarios de la autoridad investida por la Nación.

IX. Que la Ley de Acceso a la Información Pública es obligatoria para los poderes públicos de la República de El Salvador, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso

y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;

X. Que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica el tratamiento de datos personales para los fines establecidos en las disposiciones aplicables, por lo que los/las servidores/as públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, responsabilidad, de información a la persona titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transferencia;

XI. Que es de gran relevancia que las personas tengan conocimiento de su información que ~~de ellos~~ obra en los archivos del Sector Público a efecto de hacer uso de los derechos de acceso, rectificación, cancelación y oposición de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman;

XII. Que el Instituto de Acceso a la Información Pública es el garante de la protección de la información de carácter personal, a efecto de evitar injerencias a su vida privada, en equilibrio con los principios de Transparencia y Acceso a la Información Pública Gubernamental que se requieren para un desarrollo del Estado Democrático de Derecho;

POR TANTO

El Pleno del Instituto de Acceso a la Información Pública de la República de El Salvador, emite los siguientes:

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES PARA LAS INSTITUCIONES QUE CONFORMAN EL SECTOR PÚBLICO

Capítulo I

Disposiciones generales

Artículo 1.- Objeto y ámbito de aplicación

Los presentes Lineamientos establecen las políticas generales que deberán observar las dependencias y entidades de la Administración Pública para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales con el propósito de:

a. Asegurar su adecuado tratamiento e impedir su uso para finalidades distintas de aquellas que motivaron su suministro.

b. Evitar la transferencia de datos personales que sea ilícita y lesiva para la dignidad y derechos de la persona afectada.

c. Instar a la Administración Pública a adoptar una cultura institucional y una concientización acerca de la importancia de poner en práctica los principios de acceso a la información pública y la transparencia, en equilibrio con el derecho a la protección de datos personales de las personas administradas, con las limitaciones que establece la Ley.

Artículo 2.- Elementos de los datos personales

A efecto de determinar si la información que posee un ente obligado constituye un dato personal, deberán agotarse las siguientes condiciones:

- a. Que la misma sea concerniente a una persona, identificada o identificable, y
- b. Que la información se encuentre contenida en sus archivos.

Artículo 3.- Derecho a la protección de datos personales

La protección de datos personales es el derecho autónomo, con características y dinámicas, que tiene por objeto salvaguardar el poder de disposición y el control que tiene toda persona física y jurídica con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

Se reconoce el derecho de toda persona a la protección de datos personales, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Artículo 4.- Definiciones

Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en el artículo 6 de la Ley de Acceso a la Información Pública, se entenderá por:

a. Datos Personales: Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando eso no requiera plazos o actividades desproporcionadas.

b. 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 este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; identidad de los solicitantes de información, datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física.

c. Anonimización: La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re identificación de una persona sin esfuerzos desproporcionados.

d. Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición de la persona titular, previo al tratamiento de sus datos personales, a fin de cumplir con el principio de transparencia.

e. Base de datos: es un conjunto de información de una persona, almacenada de forma estructurada y sistematizada, los cuales se pueden administrar, consultar, analizar y publicar. La base de datos puede estar alojada de manera local, bajo un servicio en la nube o un tercero (empresa privada o institución pública)

f. Consentimiento: Manifestación de voluntad, libre, inequívoca, informada y específica, de la persona titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

g. Datos de acceso restringido: Aquellos datos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública.

h. Servicios en la nube: son los servicios que facilitan el procesamiento, almacenaje y disponibilidad de información, sistemas y herramientas las cuales se acceden por medio de Internet.

i. Deber de confidencialidad: Obligación de las personas responsables de bases de datos, personal a su cargo y del personal del Instituto de Acceso a la Información Pública, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la ley, principalmente cuando se acceda a información sobre datos personales.

j. Destinatario/a: Cualquier persona física o jurídica o privada que recibe datos personales.

k. Encargado/a: se refiere a la ~~Prestador~~ prestación de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del/la responsable, trata datos personales a nombre y por cuenta de este.

l. Intermediación ~~Intermediario tecnológico~~ o proveedor ~~provisión de servicios:~~ Persona física o jurídica, pública o privada que brinda servicios en la nube, SaaS (software como un servicio), PaaS (Plataforma como un servicio), IaaS (Infraestructura como servicios) u otros servicios.

m. Estándares de seguridad: diferentes técnicas, controles y mecanismos que garantizan la seguridad para la administración, resguardo y eliminación de información, por ejemplo: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2 y SOC 3, PCI DSS.

n. Instituto: Instituto de Acceso a la Información Pública (IAIP).

o. LAIP: Ley de Acceso a la Información Pública.

p. LEPINA: Ley de Protección Integral de la Niñez y Adolescencia

q. LPA: Ley de Procedimientos Administrativos

r. NNA: Niños, Niñas y Adolescentes

s. Persona física identificable: Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

s. Responsable: Ente obligado que ~~solo~~ en solitario o en conjunto ~~con otros~~, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

t. Sistema de Registro: Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

u. Titular de los datos: Persona física o jurídica a quien le conciernen los datos personales.

v. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y/o entidades a cualquier persona distinta al quien posee la titularidad ~~Titular~~ de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

w. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transferencia.

x. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizados sobre datos personales, relacionadas, de manera enunciativa más no limitativa con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Artículo 5.- Sistema de datos personales

Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a. Físicos: Conjunto ordenado de datos personales que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b. Automatizados: Conjunto ordenado de datos personales que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II

Principios rectores de la Protección de los Datos Personales

Artículo 6.- Principios aplicables

En el tratamiento de datos personales, el/la responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Artículo 7.- Principio de Legitimación

Por regla general, el tratamiento de los datos personales únicamente podrá proceder en los siguientes supuestos:

1. Cuando el/la titular otorgue su consentimiento para una o varias finalidades específicas.

2. Sea necesario para el cumplimiento de una orden judicial, resolución u orden fundada y motivada por autoridad pública competente.

3. Sea necesario para el ejercicio de facultades propias de los entes obligados o se realice en virtud de una habilitación legal.

4. Sea necesario para el reconocimiento o defensa de los derechos del/la titular ante un ente obligado.

5. Sea necesario para la ejecución de un contrato o un precontrato en el que el/la titular sea parte.

6. Resulte necesario para proteger intereses vitales del/la titular o de otra persona física.

7. Sea necesario por razones de interés público establecidas o previstas por la Ley.

Artículo 8.- Principio de Licitud

La persona responsable tratará los documentos, sistemas o registros de datos personales, que estén en su poder, con estricto apego y cumplimiento de las atribuciones legales o reglamentarias de cada ente obligado y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe de ser determinada y legítima.

Artículo 9.- Principio de Lealtad

La persona responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del quien ostenta la titularidad y absteniéndose de tratarlos a través de medios engañosos o fraudulentos.

Para estos efectos, se considerarán desleales aquellos tratamientos de datos personales que fueren contrarios al consentimiento brindado por el/la titular que den lugar a una discriminación injusta o arbitraria contra los/las titulares.

Artículo 10.- Principio de Transparencia

La persona responsable informará al/la titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

La persona responsable proporcionará al/la titular, al menos, la información siguiente:

- a. Su nombre y datos de contacto.
- b. Las finalidades del tratamiento a que serán sometidos sus datos personales.
- c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los/las destinatarios/as y las finalidades que motivan la realización de las mismas.
- d. La existencia, forma, mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación u oposición.
- e. En su caso, el origen de los datos personales cuando la persona responsable no los hubiere obtenido directamente del/la titular.

La información proporcionada al/la 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.

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

El Instituto emitirá la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.

Artículo 11.- Principio de Finalidad

Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legitimadas por la ley o normativa administrativa pertinente.

~~El~~ La persona responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

Artículo 12.- Principio de Proporcionalidad

~~El~~ La persona responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

Artículo 13.- Principio de Calidad

~~El~~ La persona responsable adoptará las medidas pertinentes para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el/la responsable por medio de la persona delegada para su tratamiento solicitará la supresión o eliminación de 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, la persona responsable implementará métodos y técnicas orientadas a la eliminación irreversible y segura de la información.

Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifican su tratamiento o aquellas relacionadas con exigencias legales aplicables a la persona responsable.

Artículo 14.- Principio de Responsabilidad

Los datos personales serán debidamente custodiados y las personas Responsables, Encargados y los titulares deberán garantizar el manejo cuidadoso en su tratamiento.

~~El~~La persona responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Lineamientos, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al/la titular y al Instituto, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Lo anterior, aplicará cuando los datos personales sean tratados por parte de una persona encargada a nombre y por cuenta del/la responsable, así como al momento de realizar transferencias de datos personales.

Entre los mecanismos que el/la responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

I. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

II. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

III. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

IV. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

V. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

VI. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

VII. Establecer procedimientos para recibir y responder dudas y quejas de los/las titulares.

La personaEl responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el

objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

Artículo 15.- Principio de Seguridad

~~El~~La persona responsable establecerá y mantendrá con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para la determinación de las medidas referidas en el numeral anterior, ~~el~~la persona responsable considerará los siguientes factores:

a) El riesgo para los derechos y libertades de los/las titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

b) Los costos de aplicación

c) La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

d) El alcance, contexto y las finalidades del tratamiento.

e) Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

f) El número de titulares.

g) Las posibles consecuencias que se derivarían de una vulneración para los/las titulares.

h) Las vulneraciones previas ocurridas en el tratamiento de datos personales.

~~El~~La persona responsable llevará 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.

Artículo 16.- Principio de Confidencialidad

~~El~~La persona responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el/la titular.

Capítulo III

Tratamiento de datos personales

Artículo 17.- Tratamiento exacto, adecuado, pertinente y no excesivo

A efecto de cumplir con el principio de calidad a que se refiere el artículo 13 de los presentes Lineamientos, se considera que el tratamiento de datos personales es:

a. Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el/la Titular de los datos se vea afectado por dicha situación;

b. Adecuado: Cuando se observan las medidas de seguridad aplicables;

c. Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y

d. No excesivo: Cuando la información solicitada a la persona Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Artículo 18.- Tratamiento de datos personales de niños, niñas y adolescentes

En el tratamiento de datos personales de niñas, niños y adolescentes, la persona responsable deberá privilegiar el interés superior de estos y la garantía de reserva, en los términos previstos en la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA) y la Convención sobre los Derechos del Niño, así como observar lo dispuesto en la LAIP.

Artículo 19.- Corrección de oficio

En caso de que las personas Responsables y Encargados detecten que hay datos personales inexactos o incompletos de conformidad al Art. 32 letra "d" de la LAIP, deberán de oficio actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Artículo 20.- Conservación de los datos

Los datos personales que hayan sido objeto de tratamiento y no contengan valor histórico, científico, estadístico o contable, deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los Lineamientos relacionados con la Gestión Documental y Archivos emitidos por este Instituto, teniendo en cuenta los siguientes plazos:

a. El que se haya establecido en el formato físico o electrónico por el cual se recabaron;

b. El establecido por las disposiciones aplicables;

- c. El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y
- d. El señalado en los casos de transferencia.

Artículo 21.- Condiciones técnicas

Los datos personales sólo podrán ser tratados en registros o sistemas de datos personales, tanto físicos como automatizados, que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Artículo 22.- Medios para recabar los datos

Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a las personas particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en los artículos 11, 15 y 16 de los presentes Lineamientos y 34 de la LAIP.

Artículo 23.- Disociación de datos

La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse a quien tiene la titularidad de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individualizada del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la normativa vigente y demás disposiciones aplicables.

Artículo 24.- Tratamiento de datos por el/la encargado/a

Cuando se contrate a una persona encargada para que realice el tratamiento de datos personales, deberá estipularse en el contrato respectivo las condiciones de utilización de los datos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, así como la determinación de responsabilidades por su incumplimiento.

Artículo 25.- Procedimientos para el tratamiento.

El La persona responsable establecerá y documentará los procedimientos para la administración, resguardo, modificación, bloqueo y supresión de los datos personales. También, determinará los mecanismos administrativos, tecnológicos y físicos para garantizar la seguridad y el acceso no autorizado a los datos personales.

~~El~~La persona responsable del tratamiento de los datos personales, debe cumplir los estándares mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales, sean estos resguardados de forma local, servicios en la nube o en servicios de instituciones públicas. Además, deberá velar por la aplicación del principio de calidad de la información.

Artículo 26.- Condiciones del tratamiento.

Corresponde a la persona responsable o al ~~encargado~~, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el/la titular, aún y cuando estos datos sean almacenados o alojados ~~por una~~ a través de intermediación ~~no~~ tecnológica.

Artículo 27.- Contratación o subcontratación de servicios.

Se podrá contratar o subcontratar los servicios de terceras personas, siempre y cuando estas cumplan con los estándares mínimos de seguridad en los servicios e infraestructura que ofrecen.

Artículo 28.- Tratamiento de datos por parte del/la encargado/a.

~~El~~La persona encargada solo podrá intervenir en el tratamiento de las bases de datos personales, según lo establecido en el contrato celebrado con el/la responsable y sus indicaciones.

Para tal efecto, la ~~el~~ persona encargada tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

- a. Tratar únicamente los datos personales conforme a las instrucciones del/la responsable;
- b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el/la responsable;
- c. Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, los presentes Lineamientos y las demás disposiciones aplicables;
- d. Guardar confidencialidad respecto de los datos personales tratados;
- e. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte de la persona responsable.

f. Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con la persona responsable o por instrucciones del responsable esta última, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Capítulo IV

Derechos de las personas Titulares y su ejercicio

Del ejercicio de los derechos de acceso, rectificación, cancelación

Artículo 29.- Derechos ARCO

En todo momento la persona titular o su representante podrán solicitar al/la responsable, el acceso, rectificación, cancelación y oposición de los datos personales que le conciernen.

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

Artículo 30.- Derecho de Acceso

De acuerdo con el Artículo 36 literales “a”, “b” y “c” de la LAIP, los/las titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, cualquier información relacionada a las condiciones generales y específicas de su tratamiento, lo siguiente:

- a. La información contenida en documentos o registros sobre su persona.
- b. Informe sobre finalidad para la que se ha recabado la información.
- c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control, en los términos del artículo 63 de la LAIP.

Artículo 31.- Alcances del Derecho de Acceso

El derecho de acceso a la información personal garantiza las siguientes facultades de la persona interesada:

- a. Obtener en intervalos razonables, según se dispone en la LAIP y en su caso en los plazos previstos en la Ley de Procedimientos Administrativos (LPA), sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.

b. Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.

c. Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al/la titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceras personas, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.

d. Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

Artículo 32.- Derecho de Rectificación

De conformidad al Artículo 36 literal “d” de la LAIP, los/las titulares de los datos personales tendrán el derecho a obtener de los entes obligados, la rectificación o corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.

Artículo 33.- Derecho de Cancelación

De conformidad al Artículo 36 literal “d” de la LAIP, los/las titulares tendrán derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, por falta de relevancia, actualidad de la información o por haberse cumplido el fin para el cual fueron recopilados; en razón de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 34.- Derecho de Oposición

De conformidad al Artículo 24 letra “b” y al Artículo 36 letra “d” de la LAIP, la persona titular podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular.

Artículo 35.- Personas facultadas para el ejercicio de los derechos ARCO

Los derechos ARCO conforme a lo establecido en los Arts. 31 y 36 de LAIP, serán ejercidos por su titular o su representante, quienes deberán acreditar su identidad al presentar su solicitud.

Artículo 36.- Ejercicio de los derechos ARCO a través de representante

Para el caso, el/la representante deberá adjuntar a su solicitud, Poder Especial en donde conste su acreditación, conforme a lo dispuesto en los Arts. 51 del Reglamento de la LAIP y 7 de los Lineamientos para la Recepción, Tramitación, Resolución y Notificación de solicitudes de acceso a la Información Pública.

Artículo 37.- Ejercicio de los derechos ARCO de las niñas, niños y adolescentes (NNA) y personas en situación de discapacidad.

Las niñas, niños y adolescentes "NNA" conforme a los Arts. 3 y 10 de la LEPINA, podrán acceder a su información personal por sí mismos o por medio de su madre, padre y otros representantes.

Los NNA menores de 14 años de edad, podrán ejercer los derechos de cancelación, rectificación y oposición a través de su madre, padre u otros representantes; en el caso de los mayores de 14 años de edad podrán ejercerlo directamente o a través de los antes mencionados, conforme lo dispuesto en los Arts. 10, 12 y 218 de la LEPINA.

En el caso, de las personas declaradas incapaces conforme a la ley, se estará a lo dispuesto en los Arts. 293 y 295 del Código Familia en lo que resulten aplicables.

Artículo 38.- Ejercicio de los derechos ARCO de personas fallecidas

Tratándose de datos personales concernientes a personas fallecidas, tendrán derecho a ejercerlos ~~aquellos~~ ~~aquellos~~ ~~quien~~ ~~que~~ acrediten un interés jurídico y podrán alegarse de manera enunciativa más no limitativa, los siguientes:

a. La parentela ~~os~~ ~~parientes~~ por consanguinidad en línea recta y en línea colateral hasta el cuarto grado de consanguinidad y en el de afinidad hasta el segundo, conforme a lo establecido en el Artículo 132 del Código de Familia.

b. La persona ~~El~~ albacea, legatario ~~o~~, heredero ~~o~~, asegurado ~~o~~ siempre y cuando el/la titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato legal y judicial para dicho efecto.

Por interés jurídico aquel que tiene una persona física que, con motivo del fallecimiento del/la titular, pretende ejercer los derechos ARCO de ésta última ~~e~~, para el reconocimiento de derechos sucesorios u otros similares.

Artículo 39.- Medios para la acreditación de la identidad de la persona titular

La persona ~~El~~ titular podrá acreditar su identidad a través de los siguientes medios:

I. Documento Único de Identidad o pasaporte

II. Otros documentos que permitan su identificación fehacientemente.

En el caso que la persona titular sea un NNA, su identidad se podrá acreditar mediante certificación de partida de nacimiento, credenciales expedidas por instituciones educativas y pasaporte. Si el/la titular es una persona en estado de incapacidad podrá acreditar su identidad por cualquiera de los documentos mencionados en este inciso; además de Documento Único de Identidad en el caso que lo posea.

Artículo 40.- Medios para la acreditación de la identidad y personalidad del/la representante

Cuando el/la titular ejerza sus derechos ARCO a través de su representante, esta última persona deberá acreditar la identidad del/la titular y su identidad y personalidad presentando ante el/la responsable lo siguiente:

I. Identificación del representante

II. Copia certificada de poder especial, en donde se le faculte específicamente para tal efecto.

Artículo 41.- Acreditación de los NNA cuando sus padres y/o madres ejerzan la representación legal

En el caso que los padres y/o madres de los NNA, pretendan ejercer los derechos ARCO de estos, además de acreditar la identidad de ellos y/o ellas en los términos descritos en el Art. 37 inciso segundo, se deberá acreditar la identidad y representación de los padres y/o madres, con los siguientes documentos:

I. Documento Único de Identidad o pasaporte, del padre y/o madre que pretenda ejercer el derecho

II. Documento legal o judicial que acredite el ejercicio de la representación legal

Artículo 42.- Acreditación de los NNA sujetos a tutela

Cuando la persona titular sea un NNA, además de acreditar la identidad de éste en los términos descritos en el Art. 37 inciso segundo, el/la tutora o representante legal deberá acreditar su identidad y representación con los siguientes documentos:

I. Documento Único de Identidad del/a tutor/a.

II. Documento legal o judicial que acredite la tutela

Artículo 43.- Acreditación del tutor de la tutela o representación legal de una persona en estado de incapacidad

Cuando el/la titular sea una persona en estado de incapacidad y se le haya nombrado tutoría o se haya decretado la prórroga o restablecimiento de la autoridad parental; además, de

acreditar la identidad de este, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

- I. Documento Único de identidad del/la tutora o representante legal
- II. Documento legal o judicial que acredite la tutela, prórroga o restablecimiento de la autoridad parental.

Artículo 44.- Acreditación de las personas vinculadas a fallecidos/as

En los términos establecido en el Art. 38 de los presentes Lineamientos, la persona que pretenda ejercer los derechos ARCO de una persona fallecida, deberá presentar la siguiente documentación:

- I. Acta de defunción de la persona titular
- II. Documento Único de Identidad de quien pretenda ejercer el derecho
- III. Documento y alegaciones que acrediten el interés jurídico que pretende ejercer.

Capítulo V

Tramitación de las solicitudes de datos personales

Artículo 45.- Solicitudes de acceso a datos personales

Para la tramitación de solicitudes de acceso información personal se estará a lo dispuesto en los artículos 36, 37, 66, 67, 68, 69, 70, 71, 72, 73 y 74 de la LAIP; al capítulo XI de su Reglamento y a lo establecido por este Instituto en el capítulo II de los Lineamientos para la recepción, tramitación, resolución y notificación de solicitudes de acceso a la información pública, en lo que fuera aplicable.

Artículo 46.- Documentos que deben acompañar las solicitudes de rectificación, cancelación y oposición de datos personales

Cuando el/la titular de los datos personales o su representante, solicite al/la oficial de información del ente obligado, la rectificación, cancelación u oposición de sus datos personales o en su caso los de su representado/a, deberán acompañar a su solicitud la documentación que respalde dicha petición; es decir, en donde conste la situación actual del dato personal, en virtud de la cual procedería una modificación, cancelación u oposición.

Artículo 47.- Plazos para la tramitación de solicitudes de acceso a datos personales

El/la Oficial de Información debe cumplir lo solicitado por el/la titular de los datos personales, tramitar de manera gratuita, y resolver en el sentido que corresponda en el plazo de diez días hábiles, contados a partir de la recepción de la solicitud o de la subsanación de la prevención, conforme a lo dispuesto en el Art. 66 de LAIP. En caso de la

rectificación, actualización, confidencialidad o supresión de la información, el plazo será de treinta días hábiles desde la presentación de la solicitud de información.

En los casos de la ampliación de los plazos en materia de solicitudes de datos personales, solo aplica para el acceso a la información personal de conformidad con el Art. 71 de la LAIP, no así para las otras peticiones enmarcadas en el Art. 36 letra “d” de la ley. Asimismo, se contabiliza el nuevo plazo desde la fecha que se da la ampliación.

Artículo 48.- Tramitación y envío de información de carácter personal por medios electrónicos

Las solicitudes de datos personales podrán ser presentadas por medio de correo electrónico, debiendo enviar el formulario o escrito correspondiente en el que conste firma o huella junto con el documento que acredite la identidad de la persona titular. Para el caso de los/las representantes, deben adjuntar los documentos que establecen estos Lineamientos, de manera escaneada u otro medio análogo.

En el caso, de la documentación que acredite la legitimación de los/las representantes, que ha sido remitida conforme al inciso anterior, deberá ser remitida de manera física al ente obligado veinticuatro horas después de haber sido enviada la solicitud, esta situación no afectará el cómputo de los plazos conforme al artículo anterior.

Capítulo VI

De la transferencia

Artículo 49.- Transferencia de los datos personales

Los entes obligados sólo podrán transferir datos personales cuando:

- a. Así lo prevea de manera expresa una disposición legal,
- b. Medie el consentimiento expreso de los/las titulares,
- c. Cuando se transmitan entre entes obligados, siempre y cuando exista una disposición legal o constitucional que lo habilite y se destinen al ejercicio específico de sus facultades.

~~El~~ La persona receptora de los datos transferidos podrá utilizarlos únicamente para los fines que motivaron la transferencia, salvo que se trate de fuentes de acceso público en general o se transfieran datos personales a organizaciones internacionales en cumplimiento a Tratados vigentes.

Artículo 50.- Deber de informar al Instituto

Los/las Oficiales de Información deberán rendir informe a este Instituto, en los términos establecidos en los presentes Lineamientos, sobre las transferencias totales o parciales de sistemas de datos personales que realice el ente obligado.

Artículo 51.- Requisitos del Informe

El informe a que hace referencia el artículo anterior deberá contener al menos, lo siguiente:

1. Identificación del Sistema de datos personales, de la persona transferente y del destinatario de los datos;
2. Finalidad de la transferencia; así como el tipo de datos que son objeto de la transferencia;
3. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por la persona transferente y destinatario;
4. Plazo por el que conservará la persona destinatario los datos que le hayan sido transferidos, el cual podrá ser ampliado mediante aviso al Instituto, y
5. Señalar si una vez concluidos los propósitos de la transferencia, los datos personales deberán ser destruidos o devueltos a la persona transferente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

Capítulo VII

De la Seguridad de los Sistemas de Datos Personales

Artículo 52.- Medidas de seguridad

Para proveer seguridad a los sistemas de datos personales, los/las titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

- a. Designar al área responsable de acuerdo a la normativa aplicable a cada ente, las cuales deben tener conocimiento sobre la materia;
- b. Proponer, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos, conforme al Art. 32 letra "e" de la LAIP;
- c. Proponer la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y

d. Proponer la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a todo el personal y ~~usuarios~~ población usuaria.

Lo dispuesto en el literal "b" debe ser remitido al Instituto para dar cumplimiento al Art. 35 de la LAIP.

Artículo 53.- Acciones sobre seguridad

En cada dependencia o entidad, se designará una Comisión o Comité interdisciplinario que coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales tanto físicos como electrónicos, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Artículo 54.- Reserva de la información

Los entes obligados conforme a lo establecido en el Art. 28 del Reglamento de la LAIP, podrán proponer la reserva de la documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica siempre y cuando coincida con alguna de las causales del Art. 19 y de los requisitos establecidos en el Art. 21 de la LAIP.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales, así como del contenido de éstos.

Artículo 55.- Resguardo de sistemas de datos personales físico y electrónico

La persona ~~El~~ Responsable deberá:

a. Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

b. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a las personas ~~Encargadas~~, área responsable y ~~usuarios~~ población usuaria titulares de los datos personales, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico,

c. Informar al Comité los nombres de las personas ~~os~~ ~~Encargadas~~ y población usuaria ~~os~~ titulares de los datos personales.

d. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;

e. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales debiendo registrarse para ello en una bitácora;

f. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en los presentes Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

g. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a la población usuaria ~~de usuarios~~ ~~que utilizan~~ ~~datos personales~~, considerando al menos las siguientes actividades:

- Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y

- Verificar y llevar un registro del contenido del equipo para facilitar los reportes de la personal Usuario que lo recibe o lo entrega para su baja.

h. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;

i. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia; y

j. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Artículo 56.- Seguridad en la red

En relación con los aspectos de seguridad, al utilizar la red de comunicación donde se transfieran datos personales, será obligatorio para los entes obligados establecer:

- a. Procedimientos de control de acceso a la red que consideren perfiles de usuarios/as o grupos de usuarios/as para el acceso restringido a las funciones y programas de los Sistema de datos personales;

- b. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los sistemas de datos personales.

Artículo 57.- Documento de seguridad

Los entes obligados, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirá un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los/las servidores/as públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Artículo 58.- Requisitos mínimos del documento de seguridad

El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

- a. El nombre, cargo y adscripción de las personas Responsables, Encargados, Área Responsable y población usuarias;
- b. Estructura y descripción de los registros y sistemas de datos personales;
- c. Especificación detallada del tipo de datos personales contenidos en el sistema;
- d. Funciones y obligaciones de los/las servidores/as públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;
- e. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos,
- f. Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja a la población usuarias y claves de acceso para la operación del sistema o registros de datos personales;
- g. Actualización de información contenida en el registro o sistema de datos personales;
- h. Procedimientos de creación de copias de respaldo y de recuperación de los datos;
- i. Bitácoras de acciones llevadas a cabo en el registro o sistema de datos personales;
- j. Procedimiento de notificación, gestión y respuesta ante incidentes; y
- k. Procedimiento para la cancelación del registro o sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Artículo 59.- Registro de incidentes

El área responsable deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Artículo 60.- Accesos controlados y bitácoras

En cada acceso a un registro o sistema de datos personales deberá guardarse como mínimo:

- a. Datos completos de la persona Responsable, Encargada o Usuario;
- b. Modo de autenticación de la persona Responsable, Encargada o Usuario;
- c. Fecha y hora en que se realizó el acceso, o se intentó el mismo;
- d. Registro o sistema de datos personales accedido;
- e. Operaciones o acciones llevadas a cabo dentro del registro o sistema de datos personales; y
- f. Fecha y hora en que se realizó la salida del registro o sistema de datos personales.

Artículo 61.-Operaciones de acceso, actualización, respaldo y recuperación

En las actividades relacionadas con la operación de los registros o sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:

- a. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente ~~los~~ las personas Responsables, Encargadas o Usuarios de los registros o sistemas de datos personales;
- b. Llevar control de los registros y sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios/as, incidentes y accesos, así como la transferencia de datos y sus destinatarios/as, de acuerdo con las políticas internas que establezca la dependencia o entidad;
- c. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios/as o grupos de usuarios/as para el acceso restringido a las funciones y programas de los sistemas de datos personales;
- d. Mecanismos de auditoría o rastreabilidad de operaciones;
- e. Garantizar que el personal que trata datos personales, sólo tenga acceso a las funciones autorizadas de los registros o sistema de datos personales según su perfil de Usuario/a;
- f. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;

g. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;

h. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los registros o sistemas de datos personales;

i. Garantizar que durante la transferencia de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;

j. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;

k. En los casos en que la operación sea externa, convenir con la persona encargada del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;

l. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;

m. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente respecto de medidas técnicas establecidas en los presentes Lineamientos y en su caso, remitirlos al Órgano Interno de Control, y;

n. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el capítulo II de los presentes Lineamientos.

Estas medidas deberán ser integradas como anexos técnicos al documento de seguridad mencionado en el Artículo 38 de los presentes Lineamientos.

Capítulo VIII

Registro del Sistema de datos personales

Artículo 62.-

Las personas Responsables deberán registrar e informar al Instituto, en un primer momento, dentro de los primeros diez días hábiles de enero y, una segunda vez, dentro de los primeros diez días hábiles de julio de cada año, lo siguiente:

a. Los registros y sistemas de datos personales;

b. Cualquier modificación sustancial o cancelación de dichos registros o sistemas, y;

c. Cualquier transferencia de registros o sistemas de datos personales de conformidad a lo dispuesto en los presentes Lineamientos.

No obstante lo anterior, en caso de existir modificación sustancial en cualquiera de los supuestos anteriores, la persona ~~el~~ Responsable deberá informar de manera inmediata al Instituto.

Artículo 63.- Datos del registro

Los registros o sistema de datos personales deberán contener, los siguientes datos:

- a. Nombre del registro o sistema;
- b. Unidad administrativa en la que se encuentra el registro o sistema;
- c. Nombre del área responsable del registro o sistema;
- d. Cargo de la jefatura ~~de~~ del área responsable;
- e. Teléfono y correo electrónico de la jefatura ~~de~~ del área responsable;
- f. Finalidad del registro o sistema, y
- g. Normatividad aplicable al registro o sistema.

El Instituto otorgará a la persona Responsable un folio de identificación por cada Sistema de datos personales registrado.

Artículo 64.- Resolución de Inscripción

Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema "persona", a efecto de dar cumplimiento a lo establecido en los Art. 35 de la LAIP.

Capítulo VII

Del Instituto

Artículo 65.- Atribuciones

Son atribuciones del Instituto, además de las otras que le impongan la Ley u otras normas, las siguientes en materia de protección de datos personales:

- a. Velar por el cumplimiento de la normativa en materia de protección de datos.
- b. Llevar un registro que contenga una lista actualizada de los registros y sistemas de datos personales conforme al Art. 35 de la LAIP.

c. Requerir a la persona responsable los documentos mencionados en los presentes Lineamientos

d. Acceder a los registros, sistemas o documentos de datos personales reguladas por los presentes Lineamientos, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante el Instituto, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

e. Resolver sobre las denuncias en materia de datos personales, conforme a las infracciones establecidas en el Art. 76 de la LAIP; además de los artículos 71 y 150 de la LPA.

f. Ordenar de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de la información contenida en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales.

g. Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.

h. Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.

i. Fomentar entre ~~los habitantes~~ la población el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

j. Emitir la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.

k. Formar y capacitar, a través de la Unidad de Capacitaciones y Formación de este Instituto, sobre materia de protección de datos personales.

En el ejercicio de sus atribuciones, el Instituto deberá emplear procedimientos automatizados de acuerdo con las mejores herramientas tecnológicas a su alcance.

Las dependencias y entidades deberán permitir a los/las servidores/as públicos del Instituto o a terceras personas ~~terceros~~ previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los registros o sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la ley, su reglamento, los presentes Lineamientos y las demás leyes relacionadas al tema.

Capítulo VII

Disposiciones transitorias

Artículo 66.- Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los/las Titulares de los mismos; es decir, sobre la finalidad de los registros o sistema de datos personales, deberán ser elaborados en términos de los presentes Lineamientos y deberán comenzar a utilizarse, a más tardar en un plazo de un año a partir de la vigencia de los presentes Lineamientos.

Artículo 67.- En tanto y a más tardar dentro de un mes, siguiente a la entrada en vigor de los presentes Lineamientos, las dependencias y entidades que recaben datos personales deberán informar a los/las Titulares de los mismos, un documento por separado en el que se detalle los propósitos para los cuales éstos se recaban.

Artículo 68.- El cumplimiento de las disposiciones contenidas en los presentes Lineamientos deberá efectuarse a más tardar en un plazo de seis meses posterior a su entrada en vigor.

En el caso del documento de seguridad y registros o sistemas de bases de datos a la cual se refiere el Lineamiento en los capítulos VII y VIII, su cumplimiento deberá efectuarse en un plazo de un año posterior a su entrada en vigor.

Artículo 69.- El Instituto deberá efectuar las siguientes acciones:

a. Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes Lineamientos y el manual de protección de datos, en un plazo máximo de tres meses a partir de la publicación de este último.

b. Elaborar las recomendaciones sobre las medidas de seguridad que se mencionan en los presentes Lineamientos, a más tardar en un plazo de tres meses a partir de su entrada en vigor.

Capítulo VIII

Disposiciones finales

Artículo 70.- Los presentes Lineamientos entrarán en vigor seis meses después de su publicación en el Diario Oficial.

Artículo 71.- Así lo acordaron por unanimidad las y los Comisionados del Instituto de Acceso a la Información Pública.-



La infrascrita Directora Ejecutiva, del Instituto de Acceso a la Información Pública, hace constar que: en el acta número cinco de sesión extraordinaria de fecha dos de abril de dos mil veinte, se acordó en el punto cuatro de dicha acta lo que se transcribe a continuación: **"PUNTO CUATRO: Aprobación de Lineamiento de gestión de solicitudes de información y de protección de datos personales, luego de ser revisados por la Unidad de Género: luego de una sesión de trabajo donde se revisaron los lineamientos y el chequeo por parte de la Unidad de Género, para incorporar lenguaje inclusivo; el Pleno aprobó por unanimidad el Lineamiento de gestión de solicitudes de información. En el mismo acto, el Pleno aprobó por unanimidad el Lineamiento de protección de datos personales."**.
Extiende la presente en San Salvador, a veinticuatro días del mes de junio de dos mil veinte.

Licda. Miriam Marlene Chávez Alfaro
Directora Ejecutiva



Claudia Torres <ctorres@iaip.gob.sv>

Invitación: Socialización Lineamientos PDP con UNFOP vie 31 de jul de 2020 10am - 12pm (CST) (ctorres@iaip.gob.sv)

1 mensaje

Johanna Clará <jduenas@iaip.gob.sv>

23 de julio de 2020, 9:40

Responder a: Johanna Clará <jduenas@iaip.gob.sv>

Para: ctorres@iaip.gob.sv, nrivera@iaip.gob.sv, cguevara@iaip.gob.sv

Tienes una invitación para el siguiente evento.

Socialización Lineamientos PDP con UNFOP

Cuándo vie 31 de jul de 2020 10am – 12pm Hora estándar central - El Salvador **más detalles »**

Información para unirse Unirse con Google Meet
meet.google.com/hoj-wrbx-vnz

Unirse por teléfono
+503 2113 3447 (PIN: 2175858752335)

Más números de teléfono

Calendario ctorres@iaip.gob.sv

Quién • jduenas@iaip.gob.sv- creador
• nrivera@iaip.gob.sv
• cguevara@iaip.gob.sv
• ctorres@iaip.gob.sv

¿Asistirás (ctorres@iaip.gob.sv)? **Sí - Quizás - No** Más opciones »

Invitación de Google Calendar

Has recibido este correo electrónico en la dirección ctorres@iaip.gob.sv de la cuenta porque estás suscrito para recibir invitaciones del calendario ctorres@iaip.gob.sv.

Si ya no quieres recibir estos correos, inicia sesión en <https://www.google.com/calendar/> y cambia la configuración de las notificaciones para este calendario.

Si reenvías esta invitación, los destinatarios podrían enviar una respuesta al organizador para que los añada a la lista de invitados, o invitar a otras personas independientemente del estado de su propia invitación, o cambiar tu respuesta de confirmación de asistencia. Más información.

 **invite.ics**
2K



Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

Fwd: Sobre publicaciones de lineamientos de PDP en el Diario Oficial

Chris Guevara <cguevara@iaip.gob.sv>

26 de enero de 2021, 13:13

Para: Stefany Beatriz Paniagua Pérez <spaniagua@iaip.gob.sv>

----- Forwarded message -----

De: **Chris Guevara** <cguevara@iaip.gob.sv>

Date: jue, 24 sept 2020 a las 7:46

Subject: Re: Sobre publicaciones de lineamientos de PDP en el Diario Oficial

To: Alfredo Martínez <jmartinez@iaip.gob.sv>

Buenos días, muchas gracias por la información. Quedo enterado, saludos.

El jue., 24 sept. 2020 a las 7:44, Alfredo Martínez (<jmartinez@iaip.gob.sv>) escribió:

Buenos días,

Enterado.

El mié., 23 sept. 2020 a las 16:07, Chris Guevara (<cguevara@iaip.gob.sv>) escribió:

Buenas tardes Lic.

Por este medio me permito consultar respecto a disponibilidad del presupuesto actual de la Unidad de Protección de Datos Personales (\$5,210.46 menos ejecuciones a la fecha, cantidad fija posterior a modificaciones, misma que se encuentra en el rubro 54). Ello con la finalidad de proceder a la publicación de los Lineamientos generales de protección de datos personales para instituciones del sector público en el Diario Oficial. A su vez, se solicita que de dicho presupuesto se destine la cantidad señalada en la cotización anexa a modo de proceder a dicha publicación.

Quedo atento a sus comentarios, deseándole a su vez un buen día.




--

Chris Guevara**Secretario Jurídico II**

Tel.: (503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: cguevara@iaip.gob.sv

Visítanos en:   *"Cuidemos el medio ambiente, imprima este correo solo si es necesario"*




--

Alfredo Martínez**Jefe de la Unidad Financiera**

Tel.: (503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: jmartinez@iaip.gob.sv

Visítanos en:   



"Cuidemos el medio ambiente, imprima este correo solo si es necesario"

--




Chris Guevara

Secretario Jurídico II

Tel.:(503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: cguevara@iaip.gob.sv

Visítanos en:   



"Cuidemos el medio ambiente. imprima este correo solo si es necesario"

--




Chris Guevara

Secretario Jurídico II

Tel.:(503) 2205-3800

Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88,
edificio Oca Chang, segundo nivel, San Salvador, El Salvador.

Correo Electrónico: cguevara@iaip.gob.sv

Visítanos en:   



"Cuidemos el medio ambiente. imprima este correo solo si es necesario"



MINISTERIO DE
GOBERNACIÓN

FAE MIGOB Y DT - IMPRENTA NACIONAL

N.I.T. 0614-060203-103-7 | Reg. No. 148235-6

Giro: Impresión

Cotización No. 2025

12 de septiembre de 2020

Señor (es): **MH-IAIP FONDO CIRCULANTE DE MONTO FIJO**

Atención a:

Atentamente brindo el detalle de los bienes y/o servicios a suministrar por usted(es) requerido:

CANTIDAD	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
1	CONSTANCIA DE PUBLICACIÓN de los Lineamientos de Protección de Datos Personales <i>Doc. ID No. 2105</i>	\$ 3.2500	\$ 3.25
1	Lineamientos generales de Protección de Datos Personales Emitido por el Instituto de Acceso a la Información Pública, (SE PUBLICARÁ POR UNA VEZ) 854X83. <i>Doc. ID No. 2105</i>	\$ 714.0000	\$ 714.00
Descuento (5.0%)			\$ 35.70
Subtotal			\$ 681.55
IVA			\$ 0.00
TOTAL			\$ 681.55

PRECIO INCLUYE IVA

CONDICIONES DE VENTAS EN SERVICIOS DEL DIARIO OFICIAL

El pago se puede realizar por medio de transferencia bancaria o remesa a la cuenta corriente No. 0590-058646-8 del BANCO AGRICOLA a nombre de MH/DGT/FAE/MINISTERIO DE GOBERNACION.

REQUISITOS INDISPENSABLES PARA PUBLICAR DOCUMENTOS:

1- EL DOCUMENTO ENVIADO PARA COTIZAR, NO PUEDE VARIAR CON EL ORIGINAL A PUBLICAR, EN SU TEXTO O FORMATO. DE LO CONTRARIO SERÁ NUEVAMENTE COTIZADO Y SU PRECIO PODRÁ VARIAR A LA COTIZACIÓN.

2- EL TIPO DE LETRA DE PREFERENCIA TIMES NEW ROMAN, LA FUENTE No. 12.

3- SI ES GRAN CONTRIBUYENTE, Y SU FACTURA PASA LOS \$113 DOLARES, FAVOR PRESENTAR COMPROBANTE DE RETENCION AL MOMENTO DE FACTURAR.

Datos para llenar comprobante de retención:

N.R.C. No.: 148235-6, N.I.T. No.: 0614-060203-103-7, Razón Social: Fondo de Actividades Especiales del Ministerio de Gobernación, Giro: Impresión, Dirección: 9ª. Calle Pte. Y 15 Av. Norte Edif. Ministerio de Gobernación Centro de Gobierno

NOTA: Esta cotización tiene validez durante los próximos 30 días.

La Dirección de la Imprenta Nacional hace del conocimiento que toda publicación en el Diario Oficial se procesa por transcripción directa y fiel del original, por consiguiente la institución no se hace responsable por transcripciones cuyos originales lleguen en forma ilegible y/o defectuosa y son de exclusiva responsabilidad de la persona o institución que los presentó. (Arts. 21, 22 y 23 Reglamento de la Imprenta Nacional).



Gladis Iglesias

Trámites en Línea, Diario Oficial

Imprenta Nacional

4a. Calle Poniente y 15 Av. Sur #829, San Salvador, El Salvador, Tel.: (503) 2527-7800

www.imprentanacional.gob.sv, e-mail: comercializacion@imprentanacional.gob.sv

12/09/2020 16:51

Pág. 1 de 1

DIARIO OFICIAL



DIRECTOR: Víctor Manuel Portillo Ruiz

TOMO N° 429

SAN SALVADOR, MIERCOLES 4 DE NOVIEMBRE DE 2020

NUMERO 220

La Dirección de la Imprenta Nacional hace del conocimiento que toda publicación en el Diario Oficial se procesa por transcripción directa y fiel del original, por consiguiente la institución no se hace responsable por transcripciones cuyos originales lleguen en forma ilegible y/o defectuosa y son de exclusiva responsabilidad de la persona o institución que los presentó. (Arts. 21, 22 y 23 Reglamento de la Imprenta Nacional).

SUMARIO

ORGANO LEGISLATIVO

Decretos Nos. 749, 750 y 751.-Exoneración de impuestos. 4-11

ORGANO EJECUTIVO

PRESIDENCIA DE LA REPÚBLICA

Acuerdos Nos. 412 y 413.- Se conceden gastos por el desempeño de misión oficial. 12

MINISTERIO DE GOBERNACIÓN Y DESARROLLO TERRITORIAL

RAMO DE GOBERNACIÓN Y DESARROLLO TERRITORIAL

Escritura pública, estatutos de la Asociación Juvenil Comunitaria y Acuerdo Ejecutivo No. 88 aprobándole sus estatutos y confiriéndole el carácter de persona jurídica. 13-18

MINISTERIO DE ECONOMÍA

RAMO DE ECONOMÍA

Acuerdo No. 1158.- Se modifica parcialmente el listado de incisos arancelarios no necesarios para la actividad incentivada, con sus respectivas excepciones, solicitada por la sociedad JV 619 International, Sociedad Anónima de Capital Variable. 19-23

Acuerdo No. 944.- Se modifica el Acuerdo Ejecutivo No. 1587, de fecha 11 de diciembre de 2014. 24

MINISTERIOS DE ECONOMÍA, DE AGRICULTURA Y GANADERÍA Y DE HACIENDA

RAMOS DE ECONOMÍA, DE AGRICULTURA Y GANADERÍA Y DE HACIENDA

Acuerdo No. 1155.- Se pone a disposición un segundo contingente de desabastecimiento de arroz en granza, clasificado en la fracción arancelaria 1006.10.90.00—"Otros", del SAC, por un volumen de hasta treinta y seis mil toneladas métricas, de cualquier origen fuera del área centroamericana. 25-28

MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA

RAMO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA

Acuerdos Nos. 15-0606 y 15-0714.- Nombramientos en diferentes cargos del Ministerio de Educación, Ciencia y Tecnología. 29-30

Acuerdo No. 15-0214.- Se autoriza a la Universidad Centroamericana de El Salvador, José Simeón Cañas, la ampliación de la vigencia del Acuerdo Ejecutivo No. 15-1236, de fecha 29 de septiembre de 2017. 30-31

ORGANO JUDICIAL**CORTE SUPREMA DE JUSTICIA**

Acuerdo No. 200-D.- Autorización para ejercer la profesión de abogado en todas sus ramas. 31

Acuerdo No. 298-D.- Se modifica el acuerdo número 15-D. de fecha veintiocho de enero de dos mil veinte. 31

INSTITUCIONES AUTÓNOMAS**INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA**

Lineamientos Generales de Protección de Datos Personales para las Instituciones que Conforman el Sector Público. 32-36

Lineamiento para Gestión de Solicitudes de Acceso a la Información Pública. 47-52

ALCALDÍAS MUNICIPALES

Decretos Nos. 1 y 3.- Ordenanzas Transitorias de Exención de Intereses y Multas Generadas por Deudas en Concepto de Tasas e Impuestos a favor de los municipios de Bolívar y Ciudad de Colón. 53-56

Estatutos de la Asociación de Desarrollo Comunal Altos del Molino, Cumbres del Molino y Loma Pacha y Acuerdo No. 24, emitido por la Alcaldía Municipal de Santa Ana, aprobándolos y confiriéndole el carácter de persona jurídica. 57-60

SECCION CARTELES OFICIALES**DE PRIMERA PUBLICACION**

Declaratoria de Herencia. 61

Aceptación de Herencia. 61

DE SEGUNDA PUBLICACION

Herencia Yacente. 62

DE TERCERA PUBLICACION

Título de Propiedad. 62-63

Herencia Yacente. 63

SECCION CARTELES PAGADOS**DE PRIMERA PUBLICACION**

Declaratoria de Herencia. 63-70

Aceptación de Herencia. 70-80

Título de Propiedad. 80-81

Título Supletorio. 82-86

Sentencia de Nacionalidad. 87-88

Muerte Presunta. 88

Nombre Comercial. 89

Señal de Publicidad Comercial. 89

Convocatorias. 89

Título Municipal. 90-91

Edicto de Emplazamiento. 91

INSTITUCIONES AUTONOMAS

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA

El Pleno del INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA, en ejercicio de las atribuciones legales establecidas en los artículos 3 letras "a", "b", "c" y "g"; 10; 18 y 58 letra "j" de la Ley de Acceso a la Información Pública (LAIP); y

Considerando:

- I. Que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;
- II. Que la protección a los datos personales es un derecho humano, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física identificada o identificable con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;
- III. Que los avances tecnológicos y el progreso de la sociedad de la información ofrecen a las personas herramientas que contribuyen a mejorar su calidad de vida. Asimismo, coadyuvan con el Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste. Por otra parte, las nuevas tecnologías facilitan ilimitadas posibilidades para transmitir un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;
- IV. Que, sin embargo, un tratamiento inadecuado de esas herramientas tecnológicas y de la información personal de la población puede atentar contra la privacidad, seguridad y autodeterminación informativa de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo;
- V. Que se requiere un nivel uniforme y elevado de protección de las personas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras injustificadas a sus derechos y acciones desproporcionadas con el uso de sus datos personales;
- VI. Que, en el tratamiento de los datos personales, es imperioso establecer un equilibrio entre los intereses de toda persona: del sector público, social y titulares, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que sean acordes con los fines perseguidos en sociedades democráticas;
- VII. Observando que el artículo 6 de la Constitución establece como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el orden público, la moral, el honor, y la vida privada;
- VIII. Que a su vez el acceso a la información pública está consagrado como derecho fundamental que el Estado está llamado a proteger. En este sentido, las instituciones públicas cumplen un papel fundamental en la promoción de la transparencia en su gestión, siendo el funcionariado público depositario de la autoridad investida por la Nación.
- IX. Que la Ley de Acceso a la Información Pública es obligatoria para los poderes públicos de la República de El Salvador, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;
- X. Que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica el tratamiento de datos personales para los fines establecidos en las disposiciones aplicables, por lo que los/las servidores/as públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, responsabilidad, de información a la persona titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transferencia;

- XI. Que es de gran relevancia que las personas tengan conocimiento de su información que obra en los archivos del Sector Público a efecto de hacer uso de los derechos de acceso, rectificación, cancelación y oposición de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman;
- XII. Que el Instituto de Acceso a la Información Pública es el garante de la protección de la información de carácter personal, a efecto de evitar injerencias a su vida privada, en equilibrio con los principios de Transparencia y Acceso a la Información Pública Gubernamental que se requieren para un desarrollo del Estado Democrático de Derecho;

POR TANTO

El Pleno del Instituto de Acceso a la Información Pública de la República de El Salvador, emite los siguientes:

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA LAS INSTITUCIONES QUE CONFORMAN EL SECTOR PÚBLICO

Capítulo I

Disposiciones generales

Artículo 1.- Objeto y ámbito de aplicación

Los presentes Lineamientos establecen las políticas generales que deberán observar las dependencias y entidades de la Administración Pública para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales con el propósito de:

- Asegurar su adecuado tratamiento e impedir su uso para finalidades distintas de aquellas que motivaron su suministro.
- Evitar la transferencia de datos personales que sea ilícita y lesiva para la dignidad y derechos de la persona afectada.
- Instar a la Administración Pública a adoptar una cultura institucional y una concientización acerca de la importancia de poner en práctica los principios de acceso a la información pública y la transparencia, en equilibrio con el derecho a la protección de datos personales de las personas administradas, con las limitaciones que establece la Ley.

Artículo 2.- Elementos de los datos personales

A efecto de determinar si la información que posee un ente obligado constituye un dato personal, deberán agotarse las siguientes condiciones:

- Que la misma sea concerniente a una persona, identificada o identificable, y
- Que la información se encuentre contenida en sus archivos.

Artículo 3.- Derecho a la protección de datos personales

La protección de datos personales es el derecho autónomo, con características y dinámicas, que tiene por objeto salvaguardar el poder de disposición y el control que tiene toda persona física y jurídica con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

Se reconoce el derecho de toda persona a la protección de datos personales, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Artículo 4.- Definiciones

Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en el artículo 6 de la Ley de Acceso a la Información Pública, se entenderá por:

- Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando eso no requiera plazos o actividades desproporcionadas.
- 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 este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; identidad de los solicitantes de información, datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física.
- Anonimización:** La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re identificación de una persona sin esfuerzos desproporcionados.

- d. **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición de la persona titular, previo al tratamiento de sus datos personales, a fin de cumplir con el principio de transparencia.
- e. **Base de datos:** Es un conjunto de información de una persona, almacenada de forma estructurada y sistematizada, los cuales se pueden administrar, consultar, analizar y publicar. La base de datos puede estar alojada de manera local, bajo un servicio en la nube o un tercero (empresa privada o institución pública).
- f. **Consentimiento:** Manifestación de voluntad, libre, inequívoca, informada y específica, de la persona titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.
- g. **Datos de acceso restringido:** Aquellos datos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública.
- h. **Servicios en la nube:** Son los servicios que facilitan el procesamiento, almacenaje y disponibilidad de información, sistemas y herramientas las cuales se acceden por medio de Internet.
- i. **Deber de confidencialidad:** Obligación de las personas responsables de bases de datos, personal a su cargo y del personal del Instituto de Acceso a la Información Pública, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la ley, principalmente cuando se acceda a información sobre datos personales.
- j. **Destinatario/a:** Cualquier persona física o jurídica o privada que recibe datos personales.
- k. **Encargado/a:** se refiere a la prestación de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del/la responsable, trata datos personales a nombre y por cuenta de este.
- l. **Intermediación tecnológica o provisión de servicios:** Persona física o jurídica, pública o privada que brinda servicios en la nube. SaaS (software como un servicio), PaaS (Plataforma como un servicio), IaaS (Infraestructura como servicios) u otros servicios.
- m. **Estándares de seguridad:** Diferentes técnicas, controles y mecanismos que garantizan la seguridad para la administración, resguardo y eliminación de información, por ejemplo: ISO 27001, ISO 27017, ISO 27018, SOC-1, SOC 2 y SOC 3, PCI DSS.
- n. **Instituto:** Instituto de Acceso a la Información Pública (IAIP).
- o. **LAIP:** Ley de Acceso a la Información Pública.
- p. **LEPINA:** Ley de Protección Integral de la Niñez y Adolescencia
- q. **LPA:** Ley de Procedimientos Administrativos
- r. **NNA:** Niños, Niñas y Adolescentes
- s. **Persona física identificable:** Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.
- t. **Responsable:** Ente obligado que en solitario o en conjunto, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
- u. **Sistema de Registro:** Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.
- v. **Titular de los datos:** Persona física o jurídica a quien le conciernen los datos personales.
- w. **Transmisión:** Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y/o entidades a cualquier persona distinta a quien posee la titularidad de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.
- x. **Transmisor:** Dependencia o entidad que posee los datos personales objeto de la transferencia.
- y. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizados sobre datos personales, relacionadas, de manera enunciativa más no limitativa con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Artículo 5.- Sistema de datos personales

Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

- a. **Físicos:** Conjunto ordenado de datos personales que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.
- b. **Automatizados:** Conjunto ordenado de datos personales que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II**Principios rectores de la Protección de los Datos Personales****Artículo 6.- Principios aplicables**

En el tratamiento de datos personales, el/la responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Artículo 7.- Principio de Legitimación

Por regla general, el tratamiento de los datos personales únicamente podrá proceder en los siguientes supuestos:

1. Cuando el/la titular otorgue su consentimiento para una o varias finalidades específicas.
2. Sea necesario para el cumplimiento de una orden judicial, resolución u orden fundada y motivada por autoridad pública competente.
3. Sea necesario para el ejercicio de facultades propias de los entes obligados o se realice en virtud de una habilitación legal.
4. Sea necesario para el reconocimiento o defensa de los derechos del/la titular ante un ente obligado.
5. Sea necesario para la ejecución de un contrato o un precontrato en el que el/la titular sea parte.
6. Resulte necesario para proteger intereses vitales del/la titular o de otra persona física.
7. Sea necesario por razones de interés público establecidas o previstas por la Ley.

Artículo 8.- Principio de Licitud

La persona responsable tratará los documentos, sistemas o registros de datos personales, que estén en su poder, con estricto apego y cumplimiento de las atribuciones legales o reglamentarias de cada ente obligado y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe de ser determinada y legítima.

Artículo 9.- Principio de Lealtad

La persona responsable tratará los datos personales en su posesión privilegiando la protección de los intereses de quien ostenta la titularidad y absteniéndose de tratarlos a través de medios engañosos o fraudulentos.

Para estos efectos, se considerarán desleales aquellos tratamientos de datos personales que fueren contrarios al consentimiento brindado por el/la titular que den lugar a una discriminación injusta o arbitraria contra los/las titulares.

Artículo 10.- Principio de Transparencia

La persona responsable informará al/la titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

La persona responsable proporcionará al/la titular, al menos, la información siguiente:

- a. Su nombre y datos de contacto.
- b. Las finalidades del tratamiento a que serán sometidos sus datos personales.
- c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los/las destinatarios/as y las finalidades que motivan la realización de las mismas.
- d. La existencia, forma, mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación u oposición.
- e. En su caso, el origen de los datos personales cuando la persona responsable no los hubiere obtenido directamente del/la titular.

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

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

El Instituto emitirá la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.

Artículo 11.- Principio de Finalidad

Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legitimadas por la ley o normativa administrativa pertinente.

La persona responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

Artículo 12.- Principio de Proporcionalidad

La persona responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

Artículo 13.- Principio de Calidad

La persona responsable adoptará las medidas pertinentes para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el/la responsable por medio de la persona delegada para su tratamiento solicitará la supresión o eliminación de 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, la persona responsable implementará métodos y técnicas orientadas a la eliminación irreversible y segura de la información.

Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifican su tratamiento o aquellas relacionadas con exigencias legales aplicables a la persona responsable.

Artículo 14.- Principio de Responsabilidad

Los datos personales serán debidamente custodiados y las personas responsables, encargadas y titulares deberán garantizar el manejo cuidadoso en su tratamiento.

La persona responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Lineamientos, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al/la titular y al Instituto, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Lo anterior, aplicará cuando los datos personales sean tratados por parte de una persona encargada a nombre y por cuenta del/la responsable, así como al momento de realizar transferencias de datos personales.

Entre los mecanismos que el/la responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

- I. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
- II. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
- III. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.
- IV. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.
- V. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
- VI. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- VII. Establecer procedimientos para recibir y responder dudas y quejas de los/las titulares.

La persona responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

Artículo 15.- Principio de Seguridad

La persona responsable establecerá y mantendrá con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para la determinación de las medidas referidas en el numeral anterior, la persona responsable considerará los siguientes factores:

- a) El riesgo para los derechos y libertades de los/las titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
- b) Los costos de aplicación
- c) La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

- d) El alcance, contexto y las finalidades del tratamiento.
- e) Las transferencias internacionales de datos personales que se realicen o pretendan realizar.
- f) El número de titulares.
- g) Las posibles consecuencias que se derivarían de una vulneración para los/las titulares.
- h) Las vulneraciones previas ocurridas en el tratamiento de datos personales.

La persona responsable llevará 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.

Artículo 16.- Principio de Confidencialidad

La persona responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el/la titular.

Capítulo III

Tratamiento de datos personales

Artículo 17.- Tratamiento exacto, adecuado, pertinente y no excesivo

A efecto de cumplir con el principio de calidad a que se refiere el artículo 13 de los presentes Lineamientos, se considera que el tratamiento de datos personales es:

- a. Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el/la Titular de los datos se vea afectado por dicha situación;
- b. Adecuado: Cuando se observan las medidas de seguridad aplicables;
- c. Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y
- d. No excesivo: Cuando la información solicitada a la persona Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Artículo 18.- Tratamiento de datos personales de niños, niñas y adolescentes

En el tratamiento de datos personales de niñas, niños y adolescentes, la persona responsable deberá privilegiar el interés superior de estos y la garantía de reserva, en los términos previstos en la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA) y la Convención sobre los Derechos del Niño, así como observar lo dispuesto en la LAIP.

Artículo 19.- Corrección de oficio

En caso de que las personas Responsables y Encargadas detecten que hay datos personales inexactos o incompletos de conformidad al Art. 32 letra "d" de la LAIP, deberán de oficio actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Artículo 20.- Conservación de los datos

Los datos personales que hayan sido objeto de tratamiento y no contengan valor histórico, científico, estadístico o contable, deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los Lineamientos relacionados con la Gestión Documental y Archivos emitidos por este Instituto, teniendo en cuenta los siguientes plazos:

- a. El que se haya establecido en el formato físico o electrónico por el cual se recabaron;
- b. El establecido por las disposiciones aplicables;
- c. El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y
- d. El señalado en los casos de transferencia.

Artículo 21.- Condiciones técnicas

Los datos personales sólo podrán ser tratados en registros o sistemas de datos personales, tanto físicos como automatizados, que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Artículo 22.- Medios para recabar los datos

Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a las personas particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en los artículos 11, 15 y 16 de los presentes Lineamientos y 34 de la LAIP.

Artículo 23.- Disociación de datos

La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse a quien tiene la titularidad de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individualizada del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la normativa vigente y demás disposiciones aplicables.

Artículo 24.- Tratamiento de datos por el/la encargado/a

Cuando se contrate a una persona encargada para que realice el tratamiento de datos personales, deberá estipularse en el contrato respectivo las condiciones de utilización de los datos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, así como la determinación de responsabilidades por su incumplimiento.

Artículo 25.- Procedimientos para el tratamiento.

La persona responsable establecerá y documentará los procedimientos para la administración, resguardo, modificación, bloqueo y supresión de los datos personales. También, determinará los mecanismos administrativos, tecnológicos y físicos para garantizar la seguridad y el acceso no autorizado a los datos personales.

La persona responsable del tratamiento de los datos personales, debe cumplir los estándares mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales, sean estos resguardados de forma local, servicios en la nube o en servicios de instituciones públicas. Además, deberá velar por la aplicación del principio de calidad de la información.

Artículo 26.- Condiciones del tratamiento.

Corresponde a la persona responsable o encargada, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el/la titular, aún y cuando estos datos sean almacenados o alojados a través de intermediación tecnológica.

Artículo 27.- Contratación o subcontratación de servicios.

Se podrá contratar o subcontratar los servicios de terceras personas, siempre y cuando estas cumplan con los estándares mínimos de seguridad en los servicios e infraestructura que ofrecen.

Artículo 28.- Tratamiento de datos por parte del/la encargado/a.

La persona encargada solo podrá intervenir en el tratamiento de las bases de datos personales, según lo establecido en el contrato celebrado con el/la responsable y sus indicaciones.

Para tal efecto, la persona encargada tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

- a. Tratar únicamente los datos personales conforme a las instrucciones del/la responsable;
- b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el/la responsable;
- c. Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, los presentes Lineamientos y las demás disposiciones aplicables;
- d. Guardar confidencialidad respecto de los datos personales tratados;
- e. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte de la persona responsable;
- f. Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con la persona responsable o por instrucciones de esta última, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Capítulo IV**Derechos de las personas Titulares y su ejercicio****Del ejercicio de los derechos de acceso, rectificación, cancelación****Artículo 29.- Derechos ARCO**

En todo momento la persona titular o su representante podrán solicitar al/la responsable, el acceso, rectificación, cancelación y oposición de los datos personales que le conciernen.

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

Artículo 30.- Derecho de Acceso

De acuerdo con el Artículo 36 literales "a", "b" y "c" de la LAIP, los/las titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, cualquier información relacionada a las condiciones generales y específicas de su tratamiento. lo siguiente:

- a. La información contenida en documentos o registros sobre su persona.
- b. Informe sobre finalidad para la que se ha recabado la información.
- c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control, en los términos del artículo 63 de la LAIP.

Artículo 31.- Alcances del Derecho de Acceso

El derecho de acceso a la información personal garantiza las siguientes facultades de la persona interesada:

- a. Obtener en intervalos razonables, según se dispone en la LAIP y en su caso en los plazos previstos en la Ley de Procedimientos Administrativos (LPA), sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.
- b. Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.
- c. Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al/la titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceras personas, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.
- d. Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

Artículo 32.- Derecho de Rectificación

De conformidad al Artículo 36 literal "d" de la LAIP, los/las titulares de los datos personales tendrán el derecho a obtener de los entes obligados, la rectificación o corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.

Artículo 33.- Derecho de Cancelación

De conformidad al Artículo 36 literal "d" de la LAIP, los/las titulares tendrán derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, por falta de relevancia, actualidad de la información o por haberse cumplido el fin para el cual fueron recopilados; en razón de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 34.- Derecho de Oposición

De conformidad al Artículo 24 letra "b" y al Artículo 36 letra "d" de la LAIP, la persona titular podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular.

Artículo 35.- Personas facultadas para el ejercicio de los derechos ARCO

Los derechos ARCO conforme a lo establecido en los Arts. 31 y 36 de LAIP, serán ejercidos por su titular o su representante, quienes deberán acreditar su identidad al presentar su solicitud.

Artículo 36.- Ejercicio de los derechos ARCO a través de representante

Para el caso, el/la representante deberá adjuntar a su solicitud, Poder Especial en donde conste su acreditación, conforme a lo dispuesto en los Arts. 51 del Reglamento de la LAIP y 7 de los Lineamientos para la Recepción, Tramitación, Resolución y Notificación de solicitudes de acceso a la Información Pública.

Artículo 37.- Ejercicio de los derechos ARCO de los niños, niñas y adolescentes (NNA) y personas en situación de discapacidad.

Las niñas, niños y adolescentes "NNA" conforme a los Arts. 3 y 10 de la LEPINA, podrán acceder a su información personal por sí mismos o por medio de su madre, padre y otros representantes.

Los NNA menores de 14 años de edad, podrán ejercer los derechos de cancelación, rectificación y oposición a través de su madre, padre u otros representantes; en el caso de los mayores de 14 años de edad podrán ejercerlo directamente o a través de los antes mencionados, conforme lo dispuesto en los Arts. 10, 12 y 218 de la LEPINA.

En el caso, de las personas declaradas incapaces conforme a la ley, se estará a lo dispuesto en los Arts. 293 y 295 del Código Familia en lo que resulten aplicables.

Artículo 38.- Ejercicio de los derechos ARCO de personas fallecidas

Tratándose de datos personales concernientes a personas fallecidas, tendrán derecho a ejercerlos quien acredite un interés jurídico y podrán alegarse de manera enunciativa más no limitativa, los siguientes:

- a. La parentela por consanguinidad en línea recta y en línea colateral hasta el cuarto grado de consanguinidad y en el de afinidad hasta el segundo, conforme a lo establecido en el Artículo 132 del Código de Familia.
- b. La persona albacea, legataria, heredera, asegurada siempre y cuando el/la titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato legal y judicial para dicho efecto.

Por interés jurídico aquel que tiene una persona física que, con motivo del fallecimiento del/la titular, pretende ejercer los derechos ARCO de esta última, para el reconocimiento de derechos sucesorios u otros similares.

Artículo 39.- Medios para la acreditación de la identidad de la persona titular

La persona titular podrá acreditar su identidad a través de los siguientes medios:

- I. Documento Único de Identidad o pasaporte
- II. Otros documentos que permitan su identificación fehacientemente.

En el caso que la persona titular sea un NNA, su identidad se podrá acreditar mediante certificación de partida de nacimiento, credenciales expedidas por instituciones educativas y pasaporte. Si el/la titular es una persona en estado de incapacidad, podrá acreditar su identidad por cualquiera de los documentos mencionados en este inciso; además de Documento Único de Identidad en el caso que lo posea.

Artículo 40.- Medios para la acreditación de la identidad y personalidad del/la representante

Cuando el/la titular ejerza sus derechos ARCO a través de su representante, esta última persona deberá acreditar la identidad del/la titular y su identidad y personalidad presentando ante el/la responsable lo siguiente:

- I. Identificación del representante
- II. Copia certificada de poder especial, en donde se le faculte específicamente para tal efecto.

Artículo 41.- Acreditación de los NNA cuando sus padres y/o madres ejerzan la representación legal

En el caso que los padres y/o madres de los NNA, pretendan ejercer los derechos ARCO de estos, además de acreditar la identidad de ellos y/o ellas en los términos descritos en el Art. 37 inciso segundo, se deberá acreditar la identidad y representación de los padres y/o madres, con los siguientes documentos:

- I. Documento Único de Identidad o pasaporte, del padre y/o madre que pretenda ejercer el derecho
- II. Documento legal o judicial que acredite el ejercicio de la representación legal.

Artículo 42.- Acreditación de los NNA sujetos a tutela

Cuando la persona titular sea NNA, además de acreditar la identidad de éste en los términos descritos en el Art. 37 inciso segundo, el/la tutora o representante legal deberá acreditar su identidad y representación con los siguientes documentos:

- I. Documento Único de Identidad del/a tutor/a.
- II. Documento legal o judicial que acredite la tutela.

Artículo 43.- Acreditación de la tutela o representación legal de una persona en estado de incapacidad

Cuando el/la titular sea una persona en estado de incapacidad y se le haya nombrado tutoría o se haya decretado la prórroga o restablecimiento de la autoridad parental; además, de acreditar la identidad de este, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

- I. Documento Único de identidad del/la tutora o representante legal
- II. Documento legal o judicial que acredite la tutela, prórroga o restablecimiento de la autoridad parental.

Artículo 44.- Acreditación de las personas vinculadas a fallecidos/as

En los términos establecido en el Art. 38 de los presentes Lineamientos, la persona que pretenda ejercer los derechos ARCO de una persona fallecida, deberá presentar la siguiente documentación:

- I. Acta de defunción de la persona titular
- II. Documento Único de Identidad de quien pretenda ejercer el derecho
- III. Documento y alegaciones que acrediten el interés jurídico que pretende ejercer.

Capítulo V**Tramitación de las solicitudes de datos personales****Artículo 45.- Solicitudes de acceso a datos personales**

Para la tramitación de solicitudes de acceso a la información personal se estará a lo dispuesto en los artículos 36, 37, 66, 67, 68, 69, 70, 71, 72, 73 y 74 de la LAIP; al capítulo XI de su Reglamento y a lo establecido por este Instituto en el capítulo II de los Lineamientos para la recepción, tramitación, resolución y notificación de solicitudes de acceso a la información pública, en lo que fuera aplicable.

Artículo 46.- Documentos que deben acompañar las solicitudes de rectificación, cancelación y oposición de datos personales

Cuando el/la titular de los datos personales o su representante, solicite al/la oficial de información del ente obligado, la rectificación, cancelación u oposición de sus datos personales o en su caso los de su representado/a, deberán acompañar a su solicitud la documentación que respalde dicha petición; es decir, en donde conste la situación actual del dato personal, en virtud de la cual procedería una modificación, cancelación u oposición.

Artículo 47.- Plazos para la tramitación de solicitudes de acceso a datos personales

El/la Oficial de Información debe cumplir lo solicitado por el/la titular de los datos personales, tramitar de manera gratuita, y resolver en el sentido que corresponda en el plazo de diez días hábiles, contados a partir de la recepción de la solicitud o de la subsanación de la prevención, conforme a lo dispuesto en el Art. 66 de LAIP. En caso de la rectificación, actualización, confidencialidad o supresión de la información, el plazo será de treinta días hábiles desde la presentación de la solicitud de información.

En los casos de la ampliación de los plazos en materia de solicitudes de datos personales, solo aplica para el acceso a la información personal de conformidad con el Art. 71 de la LAIP, no así para las otras peticiones enmarcadas en el Art. 36 letra "d" de la ley. Asimismo, se contabiliza el nuevo plazo desde la fecha que se da la ampliación.

Artículo 48.- Tramitación y envío de información de carácter personal por medios electrónicos

Las solicitudes de datos personales podrán ser presentadas por medio de correo electrónico, debiendo enviar el formulario o escrito correspondiente en el que conste firma o huella junto con el documento que acredite la identidad de la persona titular. Para el caso de los/las representantes, deben adjuntar los documentos que establecen estos Lineamientos, de manera escaneada u otro medio análogo.

En el caso, de la documentación que acredite la legitimación de los/las representantes, que ha sido remitida conforme al inciso anterior, deberá ser remitida de manera física al ente obligado veinticuatro horas después de haber sido enviada la solicitud, esta situación no afectará el cómputo de los plazos conforme al artículo anterior.

Capítulo VI**De la transferencia****Artículo 49.- Transferencia de los datos personales**

Los entes obligados sólo podrán transferir datos personales cuando:

- a. Así lo prevea de manera expresa una disposición legal,
- b. Medie el consentimiento expreso de los/las titulares,
- c. Cuando se transmitan entre entes obligados, siempre y cuando exista una disposición legal o constitucional que lo habilite y se destinen al ejercicio específico de sus facultades.

La persona receptora de los datos transferidos podrá utilizarlos únicamente para los fines que motivaron la transferencia, salvo que se trate de fuentes de acceso público en general o se transfieran datos personales a organizaciones internacionales en cumplimiento a Tratados vigentes.

Artículo 50.- Deber de informar al Instituto

Los/las Oficiales de Información deberán rendir informe a este Instituto, en los términos establecidos en los presentes Lineamientos, sobre las transferencias totales o parciales de sistemas de datos personales que realice el ente obligado.

Artículo 51.- Requisitos del Informe

El informe a que hace referencia el artículo anterior deberá contener al menos, lo siguiente:

1. Identificación del Sistema de datos personales, de la persona transferente y destinataria de los datos;
2. Finalidad de la transferencia; así como el tipo de datos que son objeto de la transferencia;
3. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por la persona transferente y destinataria;
4. Plazo por el que conservará la persona destinataria los datos que le hayan sido transferidos, el cual podrá ser ampliado mediante aviso al Instituto, y
5. Señalar si una vez concluidos los propósitos de la transferencia, los datos personales deberán ser destruidos o devueltos a la persona transferente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

Capítulo VII

De la Seguridad de los Sistemas de Datos Personales

Artículo 52.- Medidas de seguridad

Para proveer seguridad a los sistemas de datos personales, los/las titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

- a. Designar al área responsable de acuerdo a la normativa aplicable a cada ente, las cuales deben tener conocimiento sobre la materia;
- b. Proponer, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos, conforme al Art. 32 letra "e" de la LAIP;
- c. Proponer la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y
- d. Proponer la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a todo el personal y población usuaria.

Artículo 53.- Acciones sobre seguridad

En cada dependencia o entidad, se designará una Comisión o Comité interdisciplinario que coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales tanto físicos como electrónicos, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Artículo 54.- Reserva de la información

Los entes obligados conforme a lo establecido en el Art. 28 del Reglamento de la LAIP, podrán proponer la reserva de la documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica siempre y cuando coincida con alguna de las causales del Art. 19 y de los requisitos establecidos en el Art. 21 de la LAIP.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales, así como del contenido de éstos.

Artículo 55.- Resguardo de sistemas de datos personales físico y electrónico

La persona responsable deberá:

- a. Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;
- b. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a las personas encargadas, área responsable y población usuaria titular de los datos personales, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico.
- c. Informar al Comité los nombres de las personas encargadas y población usuaria titular de los datos personales.

- d. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;
- e. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales debiendo registrarse para ello en una bitácora;
- f. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en los presentes Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;
- g. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a la población usuaria que utiliza datos personales, considerando al menos las siguientes actividades:
 - Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura; y
 - Verificar y llevar un registro del contenido del equipo para facilitar los reportes de la persona Usuaria que lo recibe o lo entrega para su baja.
- h. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;
- i. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia; y
- j. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además realizar respaldos que permitan garantizar la continuidad de la operación.

Artículo 56.- Seguridad en la red

En relación con los aspectos de seguridad, al utilizar la red de comunicación donde se transfieran datos personales, será obligatorio para los entes obligados establecer:

- a. Procedimientos de control de acceso a la red que consideren perfiles de usuarios/as o grupos de usuarios/as para el acceso restringido a las funciones y programas de los Sistema de datos personales;
- b. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los sistemas de datos personales.

Artículo 57.- Documento de seguridad

Los entes obligados, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirá un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los/las servidores/as públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Artículo 58.- Requisitos mínimos del documento de seguridad

El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

- a. El nombre, cargo y adscripción de las personas Responsables, Encargadas, Área Responsable y población usuaria;
- b. Estructura y descripción de los registros y sistemas de datos personales;
- c. Especificación detallada del tipo de datos personales contenidos en el sistema;
- d. Funciones y obligaciones de los/las servidores/as públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;
- e. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos,
- f. Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja a la población usuaria y claves de acceso para la operación del sistema o registros de datos personales;
- g. Actualización de información contenida en el registro o sistema de datos personales;
- h. Procedimientos de creación de copias de respaldo y de recuperación de los datos;
- i. Bitácoras de acciones llevadas a cabo en el registro o sistema de datos personales;
- j. Procedimiento de notificación, gestión y respuesta ante incidentes; y
- k. Procedimiento para la cancelación del registro o sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Artículo 59.- Registro de incidentes

El área responsable deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Artículo 60.- Accesos controlados y bitácoras

En cada acceso a un registro o sistema de datos personales deberá guardarse como mínimo:

- a. Datos completos de la persona Responsable, Encargada o Usuaria;
- b. Modo de autenticación de la persona Responsable, Encargada o Usuaria;
- c. Fecha y hora en que se realizó el acceso, o se intentó el mismo;
- d. Registro o sistema de datos personales accedido;
- e. Operaciones o acciones llevadas a cabo dentro del registro o sistema de datos personales; y
- f. Fecha y hora en que se realizó la salida del registro o sistema de datos personales.

Artículo 61.- Operaciones de acceso, actualización, respaldo y recuperación

En las actividades relacionadas con la operación de los registros o sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:

- a. Contar con el tratamiento de datos personales que deberán observar obligatoriamente las personas Responsables, Encargadas o Usuarías de los registros o sistemas de datos personales;
- b. Llevar control de los registros y sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios/as, incidentes y accesos, así como la transferencia de datos y sus destinatarios/as, de acuerdo con las políticas internas que establezca la dependencia o entidad;
- c. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios/as o grupos de usuarios/as para el acceso restringido a las funciones y programas de los sistemas de datos personales;
- d. Mecanismos de auditoría o rastreabilidad de operaciones;
- e. Garantizar que el personal que trata datos personales, sólo tenga acceso a las funciones autorizadas de los registros o sistema de datos personales según su perfil de Usuario/a;
- f. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;
- g. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;
- h. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los registros o sistemas de datos personales;
- i. Garantizar que durante la transferencia de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;
- j. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;
- k. En los casos en que la operación sea externa, convenir con la persona encargada del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;
- l. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;
- m. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente, respecto de medidas técnicas establecidas en los presentes Lineamientos y en su caso, remitirlos al Órgano Interno de Control, y;
- n. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el capítulo II de los presentes Lineamientos.

Capítulo VIII**Registro del Sistema de datos personales****Artículo 62.**

Las personas Responsables deberán registrar e informar al Instituto, en un primer momento, dentro de los primeros diez días hábiles de enero y, una segunda vez, dentro de los primeros diez días hábiles de julio de cada año, lo siguiente:

- a. Los registros y sistemas de datos personales;

- b. Cualquier modificación sustancial o cancelación de dichos registros o sistemas, y;
- c. Cualquier transferencia de registros o sistemas de datos personales de conformidad a lo dispuesto en los presentes Lineamientos.

No obstante lo anterior, en caso de existir modificación sustancial en cualquiera de los supuestos anteriores, la persona Responsable deberá informar de manera inmediata al Instituto.

Artículo 63.- Datos del registro

Los registros o sistema de datos personales deberán contener, los siguientes datos:

- a. Nombre del registro o sistema;
- b. Unidad administrativa en la que se encuentra el registro o sistema;
- c. Nombre del área responsable del registro o sistema;
- d. Cargo de la jefatura del área responsable;
- e. Teléfono y correo electrónico de la jefatura del área responsable;
- f. Finalidad del registro o sistema, y
- g. Normatividad aplicable al registro o sistema.

El Instituto otorgará a la persona Responsable un folio de identificación por cada Sistema de datos personales registrado.

Artículo 64.- Resolución de Inscripción

Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet a efecto de dar cumplimiento a lo establecido en los Art. 35 de la LAIP.

Capítulo IX Del Instituto

Artículo 65.- Atribuciones

Son atribuciones del Instituto, además de las otras que le impongan la Ley u otras normas, las siguientes en materia de protección de datos personales:

- a. Velar por el cumplimiento de la normativa en materia de protección de datos.
- b. Llevar un registro que contenga una lista actualizada de los registros y sistemas de datos personales conforme al Art. 35 de la LAIP.
- c. Requerir a la persona responsable los documentos mencionados en los presentes Lineamientos
- d. Acceder a los registros, sistemas o documentos de datos personales regulados por los presentes Lineamientos, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante el Instituto, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.
- e. Resolver sobre las denuncias en materia de datos personales, conforme a las infracciones establecidas en el Art. 76 de la LAIP; además de los artículos 71 y 150 de la LPA.
- f. Ordenar de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de la información contenida en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales.
- g. Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
- h. Dictar las directrices necesarias, las cuales deberán ser publicadas en el Diario Oficial, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
- i. Fomentar entre la población el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.
- j. Emitir la normativa correspondiente para el contenido y alcances de los avisos de privacidad, a que se refiere los presentes Lineamientos.
- k. Formar y capacitar, a través de la Unidad de Formación de este Instituto, sobre materia de protección de datos personales.

En el ejercicio de sus atribuciones, el Instituto deberá emplear procedimientos automatizados de acuerdo con las mejores herramientas tecnológicas a su alcance.

Las dependencias y entidades deberán permitir a los/las servidores/as públicos del Instituto o a terceras personas previamente designadas por éste, el acceso a los lugares en los que se encuentran y operan los registros o sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la ley, su reglamento, los presentes Lineamientos y las demás leyes relacionadas al tema.

Capítulo X

Disposiciones transitorias

Artículo 66.- Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los/las Titulares de los mismos; es decir, sobre la finalidad de los registros o sistema de datos personales, deberán ser elaborados en términos de los presentes Lineamientos y deberán comenzar a utilizarse, a más tardar en un plazo de seis meses a partir de la vigencia de los presentes Lineamientos.

Artículo 67.- En tanto y a más tardar dentro de seis meses, siguiente a la entrada en vigor de los presentes Lineamientos, las dependencias y entidades que recaben datos personales deberán informar a los/las Titulares de los mismos, un documento por separado en el que se detalle los propósitos para los cuales éstos se recaban.

Artículo 68.- El cumplimiento de las disposiciones contenidas en los presentes Lineamientos deberá efectuarse a más tardar en un plazo de seis meses posterior a su entrada en vigor.

En el caso del documento de seguridad y registros o sistemas de bases de datos a la cual se refiere el Lineamiento en los capítulos VII y VIII, su cumplimiento deberá efectuarse en un plazo de un año posterior a su entrada en vigor.

Artículo 69.- El Instituto deberá efectuar las siguientes acciones:

- a. Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes Lineamientos, en un plazo máximo de seis meses a partir de la publicación de este último.
- b. Elaborar las recomendaciones sobre las medidas de seguridad que se mencionan en los presentes Lineamientos, a más tardar en un plazo de seis meses a partir de su entrada en vigor.

Capítulo XI

Disposiciones finales

Artículo 70.- Derogar los "Lineamientos de Protección de Datos Personales" aprobados por el Pleno del Instituto, mediante punto número seis del acta número 8/2015, emitida a las diez horas con treinta minutos del día veintitrés de febrero de dos mil quince.

Artículo 71.- Los presentes Lineamientos entrarán en vigor seis meses después de su publicación en el Diario Oficial.

Artículo 72.- Así lo acordaron por unanimidad las y los Comisionados del Instituto de Acceso a la Información Pública.

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA; San Salvador, a los dos días del mes de abril de dos mil veinte.

SILVIA CRISTINA PÉREZ SÁNCHEZ.
COMISIONADA PRESIDENTA EN FUNCIONES.

ANDRÉS GRÉGORI RODRÍGUEZ.
COMISIONADO PROPIETARIO

CLAUDIA LIDUVINA ESCOBAR CAMPOS.
COMISIONADA PROPIETARIA.

YANIRA DEL CARMEN CORTEZ ESTÉVEZ,
COMISIONADA SUPLENTE.

CESIA YOSABETH MENA REINA,
COMISIONADA SUPLENTE.

ANEXO

• Expediente Administrativo Art. 8.

Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

Los expedientes podrán tener soporte en papel o electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos; así como un índice numerado de todos los documentos que contenga, cuando fuera posible.

Cuando un trámite se refiera a un solo asunto u objeto en el que deban intervenir dos o más órganos de la Administración, se instruirá un único expediente y se resolverán todas las cuestiones al mismo tiempo, respetando los ámbitos de intervención de cada órgano o institución, conforme a sus competencias.

El Órgano que tenga la competencia para decidir el asunto emitirá la resolución final y recabará la información y autorizaciones que sean necesarias de la otra u otras instituciones a las que corresponda algún género de intervención en dicho asunto. Esto no impedirá que los interesados puedan, en tales casos, realizar por sí mismos los trámites y aportar los documentos pertinentes.

La Administración Pública deberá mantener un soporte electrónico actualizado de sus expedientes administrativos, el cual deberá ser fiel a su original y se encontrará al alcance de los interesados para su consulta, en los términos establecidos en la presente Ley. Dicho soporte electrónico, además, se utilizará en caso de reposición del original, por extravío, destrucción o inutilización. Esta medida se irá cumpliendo gradualmente, de acuerdo con los planes de implementación de las nuevas tecnologías de la información y comunicación dentro de la Administración Pública.

Para garantía de seguridad, se deberán implementar los mecanismos necesarios que salvaguarden la información y el exclusivo acceso a quienes tienen derecho en los términos establecidos en esta Ley y en las especiales que resulten aplicables.

- **Procedimiento para Aprobación de Normas Art. 162.**

La aprobación de las normas administrativas, se sujetará al siguiente procedimiento:

1. **Iniciativa.** El órgano responsable elaborará el correspondiente anteproyecto o borrador. Si la legislación sectorial así lo ha establecido, la iniciativa podrá provenir de los particulares, a quienes corresponderá presentar ante el órgano responsable, el anteproyecto o borrador de la norma;
2. **Recopilación de información.** Deberán recabarse por el órgano responsable los estudios, evaluaciones e informes de naturaleza legal, económica, medioambiental, técnica o científica que sean pertinentes. Las alegaciones realizadas por los ciudadanos serán igualmente tenidas en cuenta para encontrar la mejor solución posible;
3. **Audiencia a los ciudadanos directamente afectados en sus derechos e intereses.** La audiencia de los ciudadanos, directamente o a través de las asociaciones que les representen, se ha de producir, en todo caso, antes de la aprobación definitiva del texto normativo que les pueda afectar en sus derechos e intereses legítimos. Habrá de otorgarse un plazo razonable y suficiente, en razón de la materia y de las circunstancias concurrentes, para que esa audiencia resulte real y efectiva, pero que no podrá ser inferior a quince días. La Administración habrá de contar igualmente con un plazo razonable y suficiente para procesar y analizar las alegaciones realizadas. Podrá prescindir del trámite de consulta pública previsto en este apartado, cuando concurran razones graves de interés público o urgencia que los justifiquen, la propuesta normativa no tenga un impacto significativo en la actividad que pretende regular o no suponga la creación de obligaciones relevantes a los destinatarios. La omisión de este trámite deberá ser debidamente motivada por la autoridad competente;
4. **Participación del público.** La participación del público en general, con independencia que se vea o no afectado directamente por el proyecto de la normativa propuesta, deberá garantizarse antes de la aprobación definitiva de dicho proyecto, salvo que exista texto legal que lo prohíba. Ello podrá realizarse por los

medios que la institución tenga disponibles o a través del portal web, durante un plazo razonable que no podrá ser inferior a quince días;

5. Colaboración entre órganos y entes públicos. La administración competente para la aprobación de la norma, habrá de facilitar y recabar, mediante consulta o informes, la colaboración de los demás órganos y entes públicos, que fueren directamente afectados por la norma propuesta, o cuando le fuere requerido por un órgano que tuviere interés en ello en razón de los efectos que pueda producir la norma. Para tales efectos se otorgará un plazo razonable y suficiente, en razón de la materia y de las circunstancias concurrentes, a fin de que esa colaboración resulte real y efectiva, dicho plazo no podrá ser inferior a quince días;

6. Ponderación y motivación. El órgano regulador competente habrá de elaborar la propuesta definitiva, previa realización de una Evaluación de Impacto Regulatorio (EIR), que aplicando herramientas técnicas determine las alternativas posibles y la solución que asegure mejores beneficios para la sociedad; tomando en consideración los estudios, informes y evaluaciones que, en su caso, se hayan utilizado en el procedimiento. Además, deberá ponderar igualmente las alegaciones y los intereses invocados por los interesados, instituciones consultadas y el público en general. Antes de la aprobación definitiva, la Administración deberá motivar suficientemente las razones de las opciones que resulten elegidas, a la vista de las distintas alternativas, dejando constancia pública por cualquier medio de las ponderaciones realizadas; y,

7. Publicación. La entrada en vigor de este tipo de normas requiere su previa e íntegra publicación en el Diario Oficial. Además, teniendo en cuenta la naturaleza de la norma, el órgano administrativo competente podrá, razonadamente, utilizar otro medio de publicidad.

