

GUIA PARA TRATAMIENTO DE DATOS PERSONALES EN ADMINISTRACION PUBLICA

Acuerdo Ministerial 12
Registro Oficial 18 de 15-ago.-2019
Estado: Vigente

No. 012-2019

EL MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION

Considerando:

Que, el numeral 12 del artículo 66 de la Constitución de la República, establece: "Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley";

Que, el artículo 92 de la Constitución de la República, determina: "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados";

Que, el numeral 1 del artículo 154 de la Constitución de la República confiere a las Ministras y Ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas del área a su cargo, así como la facultad de expedir acuerdos y resoluciones administrativas;

Que, el artículo 226 de la Constitución de la República indica que: "Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";

Que, el artículo 227 ibídem dispone: "La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación";

Que, el inciso segundo del artículo 314 de la Constitución de la República, dispone que el Estado garantizará que los servicios públicos, prestados bajo su control y regulación, respondan a principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad;

Que, el artículo 4 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, establece: "Responsabilidad de la información.- Las instituciones del sector público y privado y las personas

naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información (...);

Que, la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, señala: "**Art. 6.-** Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.

También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.

La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos (...);

Que, el Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, dispone "**Art. 141.-** Utilización Datos Personales o no Personales en contenidos protegidos o no por Propiedad Intelectual.-Los datos personales o no personales que se encuentren formando parte de los contenidos protegidos o no por propiedad intelectual disponibles en bases de datos o repositorios y otras formas de almacenamiento de datos pertenecientes a personas naturales o jurídicas, sean de derecho público o privado, podrán ser utilizados exclusivamente en los siguientes casos:

- a) Cuando se trate de información clasificada como asequible;
- b) Cuando cuenten con la autorización expresa del titular de la información;
- c) Cuando estén expresamente autorizados por la ley;
- d) Cuando estén autorizados por mandato judicial u otra orden de autoridad con competencia para ello; y,
- e) Cuando lo requieran las instituciones de derecho público para el ejercicio de sus respectivas competencias o del objeto social para el que hayan sido constituidas.

No podrán disponerse de los datos personales o no personales so pretexto de los derechos de autor existentes sobre la forma de disposición de los elementos protegidos en las bases de datos.

La información contenida en las bases de datos, repositorios y otras formas de almacenamiento de datos personales o no personales son de interés público; por consiguiente, deberán ser usados con criterios equitativos, proporcionales y en su uso y transferencia deberá primar el bien común, el efectivo ejercicio de derechos y la satisfacción de necesidades sociales.";

Que, la Disposición General Vigésima Sexta del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, establece: "Las entidades públicas y personas naturales o jurídicas privadas que tengan bajo su poder documentos, datos genéticos, bancos o archivos de datos personales e informes sobre personas o sobre sus bienes, pondrán a disposición del público a través de un portal de información o página web la siguiente información y recursos:

- a) Los derechos que le asisten respecto de la protección de sus datos personales, entre ellos el derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos; y sus derechos a solicitar la rectificación,

eliminación o anulación de sus datos personales;

b) Detalle de las políticas y procedimientos institucionales para la protección de la privacidad de datos personales; y

c) Servicio de trámite en línea de las consultas y reclamos en materia de datos personales (...);

Que, la Disposición General Vigésima Séptima del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, establece: "Sin perjuicio de las excepciones previstas en la ley, el tratamiento de datos personales que incluya acciones tales como la recopilación, sistematización y almacenamiento de datos personales, requerirá la autorización previa e informada del titular.

No se requerirá de la autorización del titular cuando el tratamiento sea desarrollado por una institución pública y tenga una finalidad estadística o científica; de protección a la salud o seguridad; o sea realizado como parte de una política pública de garantía de derechos constitucionalmente reconocidos. En este caso deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares. La DINARDAP podrá solicitar que los bancos de datos personales en poder de una persona jurídica privada sean entregados a la misma con la finalidad de cumplir el presente artículo.

Que, mediante Decreto Ejecutivo No. 8 de 13 de agosto de 2009, el Presidente de la República resolvió crear el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como órgano rector del desarrollo de las Tecnologías de la Información y Comunicación, que incluye las telecomunicaciones y el espectro radio eléctrico;

Que, con Decreto Ejecutivo No. 5 de 24 de mayo de 2017, se suprime la Secretaría Nacional de la Administración Pública y se transfieren al Ministerio de Telecomunicaciones y de la Sociedad de la Información las atribuciones respecto de: "a: Gestionar la política y directrices emitidas para la gestión de la implementación del gobierno electrónico; b. Desarrollar y coordinar planes, programas o proyectos sobre gobierno electrónico que sean necesarios para su implementación";

Que, mediante Decreto Ejecutivo No. 784 de 4 de junio de 2019, el Presidente de la República nombró al licenciado Andrés Michelena Ayala, en el cargo de Ministro de Telecomunicaciones y de la Sociedad de la Información;

Que, mediante Acuerdo Ministerial No. 011-2018 de 8 de agosto de 2018, se expidió el Plan Nacional de Gobierno Electrónico para el período 2018-2021;

Que, el Plan Nacional de Gobierno Electrónico tiene como objetivo promover la participación ciudadana, la democratización de los servicios públicos, la simplificación de trámites y la gestión estatal eficiente, por medio del aprovechamiento de los recursos que actualmente posee el Estado;

Que, dentro de la Iniciativa 3, Impulsar la protección de la información y datos personales, contempla como iniciativa la emisión de normativa que permita instrumentar la protección de datos personales gestionados por la Administración Pública Central;

Que, mediante Informe Técnico de 5 de junio de 2019, aprobado por el Subsecretario de Estado -Gobierno Electrónico, se concluye: "La Guía para el tratamiento de datos personales en la Administración Pública es una de las estrategias del Plan Nacional de Gobierno Electrónico, contempladas en su programa para el fortalecimiento del Gobierno Abierto, Compromete a las entidades del Ejecutivo a articular acciones para promover la transparencia manteniendo informada a la ciudadanía sobre el tratamiento que se da a sus datos personales";

En ejercicio de las atribuciones que le confiere el numeral 1 del artículo 154 de la Constitución de la República y el artículo 17 del Estatuto del Régimen Administrativo de la Función Ejecutiva.

Acuerda:

Art. 1.- Expedir la Guía para el tratamiento de datos personales en la Administración Pública Central, que se encuentra Anexo y forma parte integral del presente Acuerdo.

Art. 2.- Disponer la implementación obligatoria de la Guía para el tratamiento de datos personales en la Administración Pública Central.

DISPOSICIONES TRANSITORIAS

Primera.- El Ministerio de Telecomunicaciones y de la Sociedad de la Información coordinará con el administrador del sistema informático "Contacto ciudadano", para que se habilite la opción para ejercer derechos de Acceso y Rectificación relacionadas con los datos personales, en un plazo de treinta (30) días, contados a partir de la suscripción del presente Acuerdo.

Segunda.- Con la finalidad de facilitar la publicación de la Política para la protección de datos personales, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, pondrá a disposición un componente tecnológico en los portales homologados, que permita la publicación de la misma, en el plazo de treinta (30) días contados a partir de la suscripción de la presente Guía, para que las entidades de la Administración Pública Central habiliten su despliegue.

Tercera.- En el plazo de noventa (90) días contados a partir de la suscripción del presente Acuerdo, las entidades de la Administración Pública Central deberán elaborar, aprobar y publicar la Política para la protección de datos personales en los diferentes canales electrónicos que disponen para interactuar con los ciudadanos.

DISPOSICION FINAL UNICA

De la ejecución, monitoreo y seguimiento de la Guía para el tratamiento de datos personales, encárguese a la Subsecretaría de Estado - Gobierno Electrónico en el ámbito de sus competencias.

El presente Acuerdo Ministerial entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dado en el Distrito Metropolitano de Quito, a 11 de junio de 2019.

f.) Lcdo. Andrés Michelena Ayala, Ministro de Telecomunicaciones y de la Sociedad de la Información.

GUIA PARA EL TRATAMIENTO DE DATOS PERSONALES EN LA ADMINISTRACION PUBLICA CENTRAL

Junio 2019

Nota: Para leer Gráficos, ver Registro Oficial 18 de 15 de Agosto de 2019, página 23.

Objeto.- La Guía para el tratamiento de datos personales en la Administración Pública Central, tiene por objeto proporcionar lineamientos para que las entidades de la Administración Pública Central (APC) mantengan informadas a las personas que acceden a través de sus canales electrónicos, sobre el tratamiento que dan a sus datos personales; y gestionen de manera adecuada los datos personales.

Ambito de aplicación.- La presente Guía es de aplicación obligatoria para todas las entidades de la Administración Pública Central, quienes deberán implementar estos lineamientos en los canales electrónicos que mantienen para comunicarse con los ciudadanos, así como a los datos que circulan y se reciben por medio de estos canales.

Términos y definiciones.- Para efectos de aplicación de la presente Guía, se consideran las siguientes definiciones:

Anonimización: Proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere.

(Reglamento General de Protección de Datos, Unión Europea, 2016/679)

APC: La Administración Pública Central comprende: la Presidencia y Vicepresidencia de la República; los ministerios de Estado; las entidades adscritas o dependientes; y, las entidades del sector público cuyos órganos de dirección estén integrados, en la mitad o más, por delegados o representantes de organismos, autoridades, funcionarios o servidores de entidades que integran la administración pública central. (Art. 45, Código Orgánico Administrativo, 2017).

Autodeterminación Informativa: es la atribución que tiene el titular de conocer y consentir sobre el uso de sus datos personales.

(Dinardap, 2019).

Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc.).

("Diccionario de términos y conceptos de la administración electrónica", Secretaría Nacional de la Administración Pública, Gobierno de España, abril 2018).

Canal electrónico: todo canal de transmisión de datos por medios electrónicos, ópticos o radiofrecuencias.

(Diccionario de términos y conceptos de la administración electrónica, Secretaría Nacional de la Administración Pública, Gobierno de España, abril 2018)

Consentimiento: toda manifestación expresa de voluntad, libre, inequívoca, específica e informada, emanada por el titular de la información o datos personales que permiten la recolección y tratamiento de los mismos.

(Diccionario de términos y Conceptos de la Administración Electrónica. Versión 4a, feb. 2019)

Cookies: es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario. Sus principales funciones son: llevar el control de usuarios, conseguir información sobre los hábitos de navegación del usuario, e intentos de acceso de programas espía. (Diccionario de términos y Conceptos de la Administración Electrónica. Versión 4a, feb. 2019)

Dato personal: dato que permite identificar o hacer identificable a un individuo directa o indirectamente.

(Reglamento General Europeo de Protección de Datos Personales, 2018)

Dato personal registrable: Es el dato personal que se encuentra en la Administración Pública, mismo que ha sido recogido de acuerdo a las facultades y atribuciones establecidas mediante norma expresa.

(Dirección Nacional de Registro de Datos Públicos, 2019)

Dato sensible: es aquel dato personal que en caso de ser tratado de manera inadecuada podría derivar en importantes riesgos para los derechos y las libertades fundamentales de una persona. Por ejemplo, ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, identificación personal, datos biométricos, condición migratoria, entre otros.

(Dirección Nacional de Registro de Datos Públicos, 2019)

Información pública: Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia

de la información tenga participación del Estado o sean concesionarios de éste.
(Lotaip, 2004)

Interoperabilidad gubernamental: Esfuerzo mancomunado y permanente de todas las entidades de la Administración Pública Central, para compartir e intercambiar entre ellas, por medio de las tecnologías de la información y comunicación, datos e información electrónicos que son necesarios en la prestación de los trámites y servicios ciudadanos que presentan las entidades, así como en la gestión interna e interinstitucional.
(Decreto Ejecutivo No. 1384, diciembre 2012)

Tratamiento de datos: Se compone de la obtención, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales.
(Dirección Nacional de Registro de Datos Públicos, 2019)

Trazabilidad: Es la capacidad para seguir la historia, aplicación o localización de todo aquello que está bajo consideración. (ISO 9000, 2005)

Vulnerabilidad: debilidad de un activo de información o control que puede ser aprovechado por una causa potencial de un incidente no deseado, el cual puede resultar en daños al sistema o a la organización.
(NTE INEN-ISO/IEC 27000:2012)

Vulneración: acción y efecto de transgredir, quebrantar, violar una ley o precepto.
(Diccionario Real Academia de la Lengua Española)

CAPITULO I DERECHO CIUDADANO A SER INFORMADO

1. Derechos que asisten al titular de los datos.- En virtud de que los datos personales identifican o hacen identificable a un individuo así como son parte del ser humano a quien se le atribuye su titularidad, resulta imprescindible que al encontrarse en registros de la Administración Pública Central, el titular tenga la facultad de ejercer los siguientes derechos y garantías que le asisten:

- a. Derecho de acceso: facultad del titular para conocer la información que se almacena en una base de datos, su origen, finalidad, criterios, tiempo de conservación y comunicación.
- b. Derecho de rectificación: facultad del titular para solicitar se rectifiquen o actualicen los datos o la información inexacta, errónea, falsa, incorrecta o imprecisa.
- c. Derecho de portabilidad: facultad del titular para recibir del responsable de datos personales, sus datos personales, en un formato compatible, actualizado, estructurado, común y mecánico.

2. Régimen de excepciones al consentimiento.- Las entidades de la APC no requieren autorización del titular, para dar tratamiento a los datos personales, en los siguientes casos:

- a. Existencia de mandato legal.
- b. Existencia de orden judicial emitida por autoridad competente.
- c. Cuando los datos son recogidos en la Administración Pública para el ejercicio de sus funciones de acuerdo con sus facultades y atribuciones.
- d. Cuando son datos de fuentes accesibles al público. Aquellos datos que se puede acceder sin necesitar el consentimiento o autorización de la persona a la que se refiere la información.
- e. En procesos de interoperabilidad o intercambio de datos entre entidades de la Administración Pública, de acuerdo con sus atribuciones.
- f. Cuando se trate de resguardar la seguridad del Estado, o en procesos de inteligencia y contrainteligencia.
- g. Cuando mantengan fines estadísticos efectuados por las entidades competentes para lo cual se

garantizará el secreto estadístico conforme las regulaciones vigentes.

h. Cuando sean utilizados en emergencias de salud pública, por entidades que sean competentes.

i. Cuando se utilicen en sucesos de desastres naturales, por entidades que sean competentes.

3. Ejercicio de derechos.- Con la finalidad de hacer efectivos los derechos anteriormente mencionados, las entidades de la APC deben incluir la Política para el tratamiento de datos personales, utilizando los mecanismos que resulten adecuados a cada medio electrónico que disponga.

4. Política para el tratamiento de datos personales.- Es un comunicado que informa de manera detallada cómo la entidad realiza el tratamiento de la información ciudadana, que se recolecta a través del canal electrónico que está siendo usado (Política de privacidad); y las condiciones a las que está sujeta el uso del canal electrónico que deben ser conocidas y aceptadas, de ser el caso, para que el titular pueda ejercer sus derechos, al tiempo que haga un buen uso del canal electrónico que está utilizando (Términos y condiciones de uso).

La Política para el tratamiento de datos personales contendrá como mínimo la siguiente información:

- El alcance: quién utiliza los datos.
- Datos que recolecta.
- La finalidad de los datos.
- Se deberá informar cuando la entidad trate información correspondiente a niñas, niños y adolescentes. Las cláusulas deberán señalar que el tratamiento respeta el interés superior y asegurar el respeto de derechos fundamentales
- El proceso para ejercer derechos de Acceso y Rectificación.
- Notificaciones en el caso de que existan cambios en la política de privacidad.
- Uso de cookies.
- Medidas para precautelar la seguridad de los datos personales.
- Base legal que sustenta el tratamiento de los datos.
- Términos y condiciones de uso.

La política debe ser elaborada acorde a las competencias y atribuciones de las instituciones. Un ejemplo de lo que debe contener la Política para el tratamiento de datos personales se encuentra en el Anexo 1, mismo que debe ser considerado como referencia.

5. Mecanismos para informar la Política para el tratamiento de datos personales.- Para que el usuario pueda informarse acerca del tratamiento de los datos personales, la entidad debe utilizar el mecanismo idóneo para informar la Política para el tratamiento de datos personales, en cada canal electrónico que disponga para comunicarse con el ciudadano.

6. Publicación de la Política para el tratamiento de datos personales en páginas web.- Las entidades deben utilizar notificaciones o ventanas emergentes visibles, las mismas que deben abarcar la siguiente información.

- Un texto que indique la aceptación expresa o no de la Política para el tratamiento de datos personales.
- El enlace al contenido de la Política para el tratamiento de datos personales.

Ver Anexo 2, mismo que debe ser considerado como referencia.

7. Proceso para ejercer derechos de Acceso y Rectificación.- La entidad debe incluir, en la Política para la protección de los datos personales, el enlace al sistema informático "Contacto ciudadano" para recibir estas solicitudes. La entidad responsable que recepte la solicitud responderá al titular de la información conforme a los procedimientos internos acorde al ordenamiento legal vigente.

CAPITULO II

TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

8. Principios.- Las entidades de la APC deben considerar los siguientes principios para el tratamiento de datos personales:

- a. Principio de consentimiento: El tratamiento de datos personales debe concebirse en base al debido sigilo y secreto; es decir, no deben divulgarse, difundirse, cederse, comercializarse o publicarse, sin que se cuente con el consentimiento del titular.
- b. Principio de calidad: Los datos personales deben ser exactos y facilitar su actualización cuando sea solicitado por el titular con el fin de evitar errores por omisión, se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- c. Principio de legalidad: Los datos personales deben ser tratados de forma lícita, leal y transparente.
- d. Principio de finalidad: Los datos personales deben ser recogidos con fines determinados y explícitos. No serán tratados ulteriormente con fines contrarios para los que fueron recogidos. Ninguno de los datos personales deberá ser utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado.
- e. Principio de proporcionalidad: Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con el tratamiento.
- f. Principio de conservación: Los datos personales deben mantenerse de manera que se permita la identificación durante no más tiempo del necesario, para los fines del tratamiento permitido de los datos personales. Deben ser eliminados, anonimizados o disociados cuando se haya cumplido con la finalidad para la cual fueron recolectados. Le corresponde a la entidad determinar las políticas para efectuar los procesos mencionados.
- g. Principio de seguridad: Los datos personales deben ser tratados de manera que se garantice la aplicación de medidas técnicas u organizativas apropiadas para evitar su pérdida, destrucción o daño accidental. En caso de vulnerarse las seguridades, el responsable deberá notificar la o las transgresiones al titular de los datos.
- h. Principio de no discriminación: El tratamiento de datos personales no puede originar discriminación de ningún tipo.

9. Actores y responsabilidades.- Para los fines de cumplimiento de la presente Guía, se determinan los siguientes actores y sus responsabilidades:

Titular de los datos: es la persona natural a quien hace referencia la información. Tiene las siguientes responsabilidades:

- Otorga el consentimiento para el tratamiento de sus datos personales.
- Realiza las correspondientes acciones para ejercer los derechos que le asisten.

Responsable de los datos: es la máxima autoridad de la institución (o su delegado). Tiene las siguientes responsabilidades:

- Aprobar la Política para el tratamiento de datos personales.
- Emitirá las directrices la aplicación y uso de la guía en la Institución.
- Garantizar los derechos y principios señalados en esta Guía.
- Designar a los responsables de atender las solicitudes de Acceso y Rectificación.

Gestor institucional: es el oficial de seguridad de la información institucional o quien haga sus veces. Le corresponde efectuar lo siguiente:

- Elaborar la Política para el tratamiento de datos personales, así como las directrices para su institución.
- Elaborar procedimientos para identificar los riesgos asociados al tratamiento de datos personales con el propósito de evaluar y/o anticipar el incumplimiento de las normas.
- Elaborar protocolos de respuesta que se anticipen a riesgos y/o acciones que conlleven violaciones de seguridad de los datos personales.
- Coordinar y dar a conocer todo lo relativo al tratamiento de datos personales dentro de su

institución.

- Determinar qué datos personales requieren trazabilidad en función de lo establecido en el Esquema Gubernamental de Seguridad de la Información respecto a la priorización de activos de información.

Encargados del tratamiento: son los funcionarios de las unidades poseedoras de la información que efectúan el tratamiento de los datos. Tienen las siguientes responsabilidades:

- Siguen directrices y disposiciones para el tratamiento de datos personales.
- Comunican al gestor institucional sobre riesgos en relación con los datos personales.
- Implementan las medidas de seguridad para proteger los datos personales.
- Implementar los criterios de trazabilidad.

10. Criterios para implementación de trazabilidad.- Las entidades determinarán qué tipo de datos personales requieren trazabilidad, en estos casos se debe considerar desde la recopilación de los datos. A continuación se detallan las acciones a implementar:

- Mantener un registro de los datos personales que han sido tratados.
- Establecer un registro de los datos personales que han sido consultados o actualizados,
- Conservar un registro de los datos que ha sido revisados o que está en proceso de revisión.

11. Criterios a considerar para nuevas soluciones informáticas.- Las entidades que van a implementar nuevas soluciones informáticas deben aplicar aspectos técnicos y operativos desde las primeras fases del diseño, en cuanto al tratamiento de datos personales, de forma que se aplique los principios de protección de datos desde el primer momento (protección de datos desde el diseño) y se garantice el ejercicio de los derechos del titular.

Asimismo, por defecto, deben garantizar que los datos personales se tratan con la mayor protección (protección de datos por defecto), de forma que los datos personales no sean accesibles a un número indefinido de personas. Solo se debe recoger los datos personales específicos para un fin determinado.

ANEXO 1

*NOTA: Este es un ejemplo referencial y debe ser adaptado a la entidad

Política para el tratamiento de datos personales en (nombre de la entidad)

En esta sección se cuenta con información sobre:

1. Alcance
2. Datos que se recolecta
3. Finalidad
4. Proceso para ejercer derecho de Acceso y Rectificación
5. Notificaciones cuando existan cambios en la política de privacidad
6. Uso de cookies
7. Medidas para precautelar la seguridad de los datos personales
8. Base legal que sustenta el tratamiento de los datos

1. Alcance

Esta política de privacidad se aplica a todos los datos personales recolectados a través de la página web institucional y de servicios de (nombre de la entidad).

En (nombre de la entidad) todos los funcionarios que realizan el tratamiento de los datos personales, suscriben acuerdos de confidencialidad de la información.

2. Datos que se recolecta

(nombre de la entidad) recopila los siguientes datos personales en línea:

- Su nombre y datos de contacto.
- Fecha de nacimiento.
- Datos de perfil en línea.
- Datos de contacto en caso de emergencia.
- Datos del perfil de las redes sociales.
- Copias de documentos de identificación.
- Educación e información profesional.
- Dispositivo que utiliza.
- Datos de autenticación.
- Datos sobre la ubicación,
- Otros datos que usted cargue o nos proporcione.

Prácticas de registro

(Nombre de la entidad) registra automáticamente las direcciones de Protocolo de Internet (IP) de los visitantes. La dirección IP es un número único asignado a cada computadora en Internet. En general, una dirección IP que cambia cada vez que se conecta a Internet es una dirección dinámica. Sin embargo, tenga en cuenta que, con algunas conexiones de banda ancha, su dirección IP es estática y podría estar asociada a su computadora personal.

Hacemos un seguimiento de las páginas visitadas en el sitio web de (nombre de la entidad), la cantidad de tiempo que pasa en esas páginas y los tipos de búsquedas realizadas en ellas. Sus búsquedas permanecen confidenciales y anónimas, (nombre de la entidad) utiliza esta información solo con fines estadísticos para averiguar qué páginas encuentran los usuarios más útiles y para mejorar el sitio web.

(Nombre de la entidad) también almacena los datos que usted transmite. Esto puede incluir:

Navegador / tipo de dispositivo / versión.

Sistema operativo utilizado.

Dirección de control de acceso a medios (MAC).

Fecha y hora de la solicitud del servidor.

Volumen de datos transferidos.

3. Finalidad

(nombre de la entidad) utiliza (y, cuando se especifica, comparte) su información personal para los siguientes fines:

- Para procesar transacciones se usa información personal como el nombre, la dirección física, el número de teléfono, la dirección de correo electrónico. Utilizamos la información financiera y de la tarjeta de crédito y de pago para procesar su pedido y es posible que debamos compartir parte de esta información con los servicios de entrega, las cámaras de compensación de tarjetas de crédito y otros terceros para completar la transacción.
- Para proporcionar soporte u otros servicios, (Nombre de la entidad) puede usar su información personal para proporcionarle asistencia u otros servicios que haya solicitado o solicitado. (Nombre de la entidad) también puede usar su información personal para responder directamente a sus solicitudes de información.
- Para proporcionar información basada en sus necesidades y responder a sus solicitudes, (Nombre de la entidad) puede usar su información personal para proporcionarle avisos de nuevos lanzamientos de productos y desarrollos de servicios.
- Para proporcionar foros en línea y redes sociales. Algunos servicios disponibles en los sitios web le permiten participaren discusiones interactivas, publicar comentarios, oportunidades u otro contenido en un tablón de anuncios o intercambio, o participar en actividades de redes.
- Para administrar servicios. (Nombre de la entidad) puede contactarlo para confirmar cierta

información (por ejemplo, que no tuvo problemas en el proceso de descarga).

- Para evaluar el uso de los productos y servicios. (Nombre de la entidad) puede rastrear el uso de los servicios para determinar su nivel de uso, y esas estadísticas son para uso exclusivo de esta entidad.

- Para comunicarnos con usted acerca de una reunión, conferencia o evento organizado o copatrocinado por (nombre de la entidad) o una de nuestras instituciones adscritas. Esto puede incluir información sobre el contenido del evento, la logística del evento, las actualizaciones y la información adicional relacionada con el evento.

- Para considerarlo para un reconocimiento o distinción.

- Para proteger contenidos y servicios. Podemos usar su información para prevenir actividades potencialmente ilegales y para hacer cumplir nuestros términos y condiciones. También utilizamos una variedad de sistemas tecnológicos para detectar y abordar actividades anómalas y para analizar el contenido a fin de evitar abusos, como el spam. Para obtener retroalimentación o aportación de usted. Con el fin de ofrecer productos y servicios de mayor interés (por ejemplo, a través de encuestas, estudios de usabilidad, grupos de enfoque).

Datos personales de niños

(Nombre de la entidad) no recopila datos de o sobre niños sin el permiso de los padres o tutores. Si nos enteramos de que hemos recopilado información personal de un niño, eliminaremos esa información lo más rápido posible. Si cree que podemos tener alguna información de o sobre un niño, contáctenos.

4. Proceso para ejercer derecho de Acceso y Rectificación

(Nombre de la entidad) reconoce a los titulares de datos personales el Acceso y Rectificación al tratamiento que se realice sobre sus datos, para lo cual debe seguir el respectivo proceso, ingresando al siguiente enlace:

<https://aplicaciones.administracionpublica.gob.ec/>

Derecho de Acceso

Indicar el procedimiento que se sigue en la entidad, partiendo de la recepción del pedido, hasta la entrega de la respuesta.

Derecho de Rectificación

En el caso de detectar errores de omisión, como errores tipográficos u ortográficos, deberá iniciar el pedido para la rectificación por el medio que sea definido por (nombre de la entidad), y deberá indicar el proceso que se sigue hasta hacer efectiva la rectificación.

(Nombre de la entidad) analiza si el pedido es procedente o no y comunica al titular notificando dicho particular.

5. Notificaciones cuando existan cambios en la política de privacidad

(Nombre de la entidad) puede actualizar su Política de Privacidad cuando sea necesario. Si realizamos cambios sustanciales, le notificaremos por correo o mediante un aviso en este sitio web antes de que el cambio entre en vigencia. Le recomendamos que revise periódicamente esta página para obtener la información más reciente sobre nuestras prácticas de privacidad.

6. Uso de cookies

(Nombre de la entidad) puede utilizar sus datos personales, incluidos los datos recopilados como resultado de la navegación del sitio y los protocolos y registros electrónicos para ayudar a crear y personalizar el contenido del sitio web, mejorar la calidad del sitio web, realizar un seguimiento de la capacidad de respuesta de los servicios entregados.

No compartimos sus datos personales sin su consentimiento. Cuando hace clic o interactúa con un anuncio, existe la posibilidad de que el anunciante pueda colocar una cookie en su navegador con sus propias condiciones de uso.

7. Medidas para precautelar la seguridad de los datos personales

(Nombre de la entidad) protege la confidencialidad, integridad y disponibilidad de los activos de información al seguir un enfoque de administración de riesgos basado en políticas, estándares, pautas y procedimientos para cumplir con los objetivos de seguridad al tiempo que respalda los objetivos.

(Nombre de la entidad) utiliza el protocolo HTTPS para brindar seguridad en el uso de este canal electrónico.

Mitiga los riesgos utilizando el ECSI, Normas ISO 27000, OWAS, etc.

8. Base legal que sustenta el tratamiento de los datos

(Nombre de la entidad) fundamenta el tratamiento que da a los datos personales en los siguientes instrumentos legales, como los que se citan a continuación.

COESCCi, Disposiciones Generales, VIGESIMA SEPTIMA.- "(...) El tratamiento de datos personales que incluya acciones tales como la recopilación, sistematización y almacenamiento de datos personales, requerirá la autorización previa e informada del titular. No se requerirá de la autorización del titular cuando el tratamiento sea desarrollado por una institución pública y tenga una finalidad estadística o científica; de protección a la salud o seguridad; o sea realizado como parte de una política pública de garantía de derechos constitucionalmente reconocidos".

Decreto Ejecutivo No. 1384, diciembre 2012, que establece como política pública el desarrollo de la interoperabilidad gubernamental que consiste en el esfuerzo mancomunado y permanente de todas las entidades de la Administración Pública Central, para compartir e intercambiar entre ellas, por medio de las tecnologías de la información y comunicación, datos e información electrónicos que son necesarios en la prestación de los trámites y servicios ciudadanos que presentan las entidades, así como en la gestión interna e interinstitucional.

El uso de este portal o de cualquiera de sus componentes, implica la aceptación expresa de los presentes Términos y condiciones de uso.

(Nombre de la entidad) dispone de este portal web para prestar información a los ciudadanos sobre la gestión que lleva adelante.

Los datos que han recibido tratamiento estadístico pueden estar disponibles en formatos abiertos, para facilitar su utilización.

Los trámites, servicios, transacciones o movimientos que se realicen después de las de las dieciocho horas o en días inhábiles, se considerarán realizados al día hábil siguiente.

Responsabilidad

(Nombre de la entidad) solamente será responsable del tratamiento y uso de los datos personales que recabe en forma directa a través de este canal electrónico (portal, teléfono, etc.).

(Nombre de la entidad) se deslinda de cualquier responsabilidad que pueda generar al usuario por cualquier uso inadecuado o contrario a los fines de este canal electrónico.

(Nombre de la entidad) no se hace responsable por la veracidad o exactitud de la información contenida en los enlaces a otros sitios web o que haya sido entregada por terceros.

Son obligaciones del usuario

- No dañar, inutilizar, modificar o deteriorar los canales electrónicos a los que está teniendo acceso, ni los contenidos incorporados y almacenados en éstos.
- No utilizar versiones de sistemas modificados con el fin de obtener accesos no autorizados a cualquier canal electrónico, contenido y/o servicios ofrecidos a través de estos.
- No interferir ni interrumpir el acceso, funcionalidad y utilización de canales electrónicos y redes conectados al mismo.

ANEXO 2

Ejemplo de ventana emergente para la aceptación de la Política para el tratamiento de datos personales

ANEXO 3

Participantes en el proceso de co-creación

Nota: Para leer Anexos, ver Registro Oficial 18 de 15 de Agosto de 2019, página 35.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION

Con Acción de Personal Nro. 163, de 12 de abril de 2019, con fecha de vigencia a partir de 15 de abril de 2019.

Esta diligencia es realizada al amparo de la atribución que le asiste, expresada en el Estatuto de Gestión Organizacional por Procesos del MINTEL, numeral 3.2.1.1. Gestión Administrativa; literal I)" Certificar los documentos y actos administrativos y normativos expedidos por la institución".

Certifica:

Fiel copia del original del ACUERDO MINISTERIAL No. 012-2019, constituido de once hojas útiles, el mismo que reposa en la Unidad de Gestión Documental.

A petición de Dra. Betty Cuarán, de la Dirección de Asesoría Legal y Desarrollo Normativo

Solicitud de Certificación No. 352

Quito, Veintiséis de julio de dos mil diecinueve.

f.) Mgs. Roberto Trujillo, Director Administrativo.