FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

La cláusula de protección de datos y las consecuencias jurídicas de su incumplimiento en el servicio de rentas internas del ecuador.

Profesor

Lorena Naranjo Godoy

Autor

Martin Fernando Randi Proaño

2024

INDICE

Resumen Ejecutivo 4

Abstract.....4

1. Introducción.....5

2. Identificación del objeto de estudio 6

3. Planteamiento del problema.....6

3.1. Problema 6

3.2. Preguntas específicas de la investigación.....7

3.3. Efectos del problema 8

3.4. Causas del problema 8

3.5. Escenarios.....8

3.6. Antecedentes de la investigación.....8

4. Objetivo general 10

4.1. Objetivo especifico.....10

5. Justificación y aplicación metodológica.....10

5.1. Justificación 11

5.2. Metodología.....12

5.3. Métodos.....13

CAPITULO 1: LOS DATOS PERSONALES.....13

1.1. Conceptualización.....13

1.2. La protección de datos personales en el Derecho internacional.....14

1.3. Reglamento General de Protección de datos personales mayor estándar de protección 16

1.4. Los datos personales en la normativa de América Latina 18

CAPITULO 2: El Derecho a la Protección de datos.....19

2.1. Definición.....19

2.2. Principios del derecho a la protección de datos personales 19

2.3. Protección de datos en Ecuador 23

CAPITULO 3: Derechos ARCOS 28
3.1. Definición 28
3.2. Bases legitimas 29
CAPITULO 4: DISCUSIÓN TEÓRICA DOCTRINARIA 31
4.1. La protección de datos personales 31
4.2 La ley orgánica de datos personales 33
4.3. El Servicio De Rentas Internas y el Derecho a los datos personales 34
4.3.1. Política de datos personales en el SRI 34
4.4. Políticas de protección de Datos 37
4.4.1. Una visión comparada de la protección de datos 37
CAPITULO 5: POLÍTICA DE DATOS PERSONALES EN EL SRI 38
CAPÍTULO 6: PROPUESTA DE POLÍTICA INTERNA PARA EL MANEJO DE DATOS PERSONALES EN EL SERVICIO DE RENTAS INTERNAS (SRI) 40
6.1. Introducción 40
6.2. Justificación 42
6.3. Propuesta 43
CAPITULO 7: CONCLUSIONES Y RECOMENDACIONES 48
7.1. Conclusiones 48
7.2. Recomendaciones 49
Bibliografía 50

Resumen Ejecutivo

El avance tecnológico y el uso masivo de datos han destacado la importancia de la protección de datos personales. En Ecuador, aunque la Constitución y la reciente Ley de Protección de Datos Personales junto a su reglamento establecen un régimen de protección, existe una notable falta de claridad sobre el manejo adecuado de los datos personales especialmente dentro del Servicio de Rentas Internas (SRI), debido a que, la política interna sobre el manejo de los datos personales del contribuyente no es una política completa que aborde todos los mecanismos, derechos y principios que garanticen el Derecho a la seguridad de los datos personales, este vacío legislativo genera inseguridad jurídica y plantea un problema significativo que merece ser investigado. Para abordar esto, se estudiarán en detalle la normativa vigente y las medidas implementadas por el SRI para la protección de datos personales, evaluando su eficacia y alcance en conformidad con los mandatos de la Constitución, la ley y su reglamento. La metodología de la investigación incluirá una revisión exhaustiva de la legislación existente, análisis de documentos relevantes respecto del derecho y protección de datos. La investigación dio como resultado una propuesta de política interna para la protección de los datos personales en vista de que la actual política que maneja el Servicio de Rentas Internas es muy general.

Palabras clave: datos personales, política interna, principios, protección, SRI.

Abstract

Technological progress and the massive use of data have highlighted the importance of personal data protection. In Ecuador, although the Constitution and the recent Personal Data Protection Law together with its regulations establish a protection regime, there is a notable lack of clarity on the proper handling of personal data especially within the Internal Revenue Service (SRI), due to the fact that, the internal policy on the handling of taxpayer's personal data is not a complete policy that addresses all the mechanisms, rights and principles that guarantee the Right to personal data security, this legislative vacuum generates legal insecurity and poses a significant problem that deserves to be investigated. To address this, the current regulations and measures implemented by the SRI for the protection of personal data will be studied in detail, evaluating their effectiveness and scope in accordance with the mandates of the Constitution, the law and its regulations. The research methodology will include a comprehensive review of existing legislation, analysis of relevant documents regarding the law and data protection. The research resulted in a proposal for an internal policy for the protection of personal data in view of the fact that the current policy managed by the Internal Revenue Service is very general.

Key words: personal data, internal policy, principles, protection, SRI.

1. Introducción

En el contexto actual de Ecuador, la implementación de soluciones digitales en los procesos gubernamentales y el creciente uso de tecnologías digitales por parte del Servicio de Rentas Internas han provocado un incremento significativo en la recolección y utilización de información personal de los contribuyentes. Esto se justifica en la legislación que busca optimizar la eficiencia de los trámites administrativos, asegurando un manejo seguro de los datos entre las instituciones, independientemente de su naturaleza o función, y es fundamental para la gestión tributaria.

La Constitución ecuatoriana establece que la comunicación y la información deben ser accesibles, diversas, inclusivas, oportunas y seguras para todos los ciudadanos. Además, garantiza el derecho a la protección de datos personales, otorgando a los individuos el control sobre su información y la correspondiente protección de la misma, requiriendo autorización para su recolección, almacenamiento, procesamiento, distribución o difusión, a menos que la ley disponga lo contrario.

La estructura organizativa del SRI, adaptada a los desafíos actuales, destaca la importancia de proteger la privacidad de los contribuyentes. En el caso de los contribuyentes, tienen la oportunidad de aceptar o rechazar el uso de sus datos cada vez que interactúan con el acuerdo de uso de medios electrónicos del SRI, ya sea a través de formularios físicos, de forma telefónica, en páginas web, mediante documentos impresos firmados, etc. Es importante destacar que los contribuyentes tienen la libertad de decidir en qué procesos desean que se utilicen sus datos y en cuáles no, aunque esto signifique que no podrán acceder a ciertos servicios de manera activa.

En el Servicio de Rentas Internas (SRI), se han establecido diversos procedimientos para aceptar los términos y condiciones en el uso de datos en entornos digitales, los cuales han sido comunicados a los contribuyentes en todos los puntos de contacto disponibles. Tanto el contribuyente como el SRI están comprometidos en recopilar únicamente la información necesaria para cumplir con sus responsabilidades tributarias, informando claramente sobre la

finalidad de la recolección de datos y solicitando el consentimiento cuando sea requerido.

El Servicio de Rentas Internas se adhiere a la normativa de la Ley Orgánica de Protección de Datos Personales, la cual regula el tratamiento y resguardo de la información personal de los contribuyentes, en esta ley se establecen los principios fundamentales que rigen la protección de datos, diferenciando entre datos privados como la dirección o número telefónico que no representan un riesgo significativo para los contribuyentes, y datos íntimos como la orientación sexual o religión que requieren consentimiento expreso debido a su sensibilidad. Es esencial que estas medidas de seguridad y protección de datos sean implementadas de forma constante en las actividades diarias del SRI, asegurando que la privacidad de los contribuyentes sea primordial en cada interacción con la institución de acuerdo con catálogo de servicios ofertados.

2. Identificación del objeto de estudio

La presenten investigación tiene como objetivo analizar y determinar la aplicación de la responsabilidad civil y penal, así como del régimen sancionatorio, por el incumplimiento de la cláusula de protección de datos en el Servicio de Rentas Internas en Ecuador. Para lograr este objetivo, se realizará un estudio de la normativa vigente en materia de protección de datos personales, así como de las posibles sanciones que se pueden aplicar en caso de incumplimiento de dicha normativa.

3. Planteamiento del problema

3.1. Problema

La protección de datos personales ha cobrado relevancia a nivel global, debido principalmente al avance tecnológico y al uso masivo de datos en distintas áreas de la sociedad. En virtud de ello, la normativa en la materia se ha expandido y consolidado poco a poco.

En el Ecuador, a pesar de que existe un régimen de protección de datos personales señalado en la Constitución y que la Ley de Protección de Datos Personales y su reglamento que entró en vigencia recientemente, se evidencia una ausencia clara respecto a las sanciones civiles o penales por su

incumplimiento, específicamente en el Servicio de Rentas Internas. Esta ausencia de claridad y certeza en torno a las posibles sanciones por el incumplimiento de la normativa en protección de datos personales constituye un problema relevante en términos de seguridad jurídica, lo que abre un espacio de interés para la investigación y el análisis jurídico.

La problemática para la investigación se establecería entonces sobre cómo se aplica la responsabilidad civil y penal, y de régimen sancionatorio por incumplimiento de la cláusula de protección de datos en el Servicio de Rentas Internas de Ecuador.

Además, es necesario analizar las medidas que ha implementado el Servicio de Rentas Internas hasta el momento en relación con la protección de datos personales, así como sus implicancias y efectos. Por lo tanto, se buscará comprender y evaluar si estas son suficientes y efectivas en cumplir con lo estipulado por la Constitución ecuatoriana, Ley de Protección de Datos Personales y su reglamento en caso de incumplimientos. ¿Cuáles serían las posibles sanciones y su impacto?

Un estudio de esta temática puede servir para ayudar a eficientizar el régimen sancionatorio aplicable, a modo de incrementar la seguridad jurídica y la protección efectiva de los derechos personales en el ámbito tributario ecuatoriano.

3.2. Preguntas específicas de la investigación

1. ¿Cuál es el marco normativo que regula la protección de datos personales en el ámbito tributario en Ecuador?
2. ¿Qué medidas concretas ha implementado el Servicio de Rentas Internas para garantizar la protección de datos personales de los contribuyentes?
3. ¿Cuál es el alcance de la responsabilidad civil y penal por el incumplimiento de la cláusula de protección de datos en el Servicio de Rentas Internas?
4. ¿Existen precedentes de sanciones aplicadas por el incumplimiento de la normativa de protección de datos en el Servicio de Rentas Internas?
5. ¿Cuál es el impacto de las sanciones previstas en caso de incumplimiento de la normativa de protección de datos en el ámbito tributario para

garantizar la seguridad jurídica y la protección de los derechos personales?

3.3. Efectos del problema

Se ha identificado varios efectos del problema, como la falta de definición en las penalizaciones por infringir las regulaciones de protección de datos en el Servicio de Rentas Internas lo cual puede ocasionar vulnerabilidades en la intimidad de los contribuyentes, incertidumbre legal, impunidad frente a violaciones de datos, riesgos de ciberseguridad y menoscabo en la reputación de la Administración Tributaria. Por tanto, es crucial abordar esta problemática a través de investigaciones que mejoren el sistema de sanciones y garanticen la protección efectiva de la información personal en el ámbito fiscal del país.

3.4. Causas del problema

La raíz del inconveniente radica en la falta de aplicación de las cláusulas de protección de datos por parte del Estado en los procedimientos pertinentes, es decir, se está tomando a la ligera las normativas destinadas a salvaguardar la privacidad del contribuyente y sus datos sensibles.

3.5. Escenarios

Con la investigación se lograría establecer con claridad las sanciones civiles y penales por incumplimiento de la normativa en protección de datos personales en el Servicio de Rentas Internas de Ecuador. Esto brindaría seguridad jurídica tanto a los ciudadanos como a las empresas que proporcionan sus datos personales a esta entidad. Además, se implementarían medidas efectivas por parte del SRI para proteger los datos personales de los contribuyentes, garantizando así el cumplimiento de lo establecido en la Constitución ecuatoriana, Ley de Protección de Datos Personales y su reglamento. Esto contribuiría a fortalecer la confianza de la ciudadanía en esta institución y en los sus diferentes procesos.

3.6. Antecedentes de la investigación

Según manifiesta (Córdoba, et. al, 2020), el derecho a la protección de datos personales se refiere al conjunto de derechos que permiten a una persona tener

el control sobre cómo se utilizan sus datos personales, ya sea en formatos físicos o digitales, especialmente en lo que respecta a aspectos íntimos o privados de su vida, añade además que;

> El derecho a la protección de datos personales está estrechamente vinculado con la dignidad humana y otros derechos fundamentales, como la intimidad, el buen nombre, el acceso a la información y la libertad. El consentimiento previo, explícito, informado, claro y verificable del titular de los datos para su tratamiento legítimo es crucial para que este pueda ejercer control sobre ellos (p. 77).

Dentro del contexto ecuatoriano (Martínez, et.al, 2023) dice que, el Estado ecuatoriano tiene la responsabilidad de asegurar la protección de los datos personales almacenados en las bases de datos de sus instituciones, ya que esta información es un objetivo de interés para delincuentes cibernéticos, tanto nacionales como internacionales, ademas añade que;

> A pesar de contar con una legislación de protección de datos personales en Ecuador, la seguridad de la información personal de los ciudadanos no está garantizada. Se necesita un cambio no solo en el aspecto legal, sino en la sociedad en general para lograr esta protección. La protección de los datos personales requiere una importante inversión económica y técnica por parte de las instituciones públicas, ya que el Estado ha demostrado ser incapaz de protegerlos (p. 24).

Los avances tecnológicos según manifiesta (Rivera, 2023), han traído beneficios a la vida de las personas, sin embargo, en Ecuador, la falta de una adecuada Ley de Protección de Datos impide garantizar el derecho de los ciudadanos a controlar su información, además menciona que;

> Ecuador no tiene una ley específica que regule el manejo de datos personales, pero esto no significa que no exista un marco legal básico para proteger a los individuos y sus datos. La Constitución de la República del Ecuador reconoce y garantiza el derecho a la protección de datos personales, incluyendo el acceso y la decisión sobre esta información, así como su protección correspondiente (p.119).

Por otro lado, (Proaño, 2021) en un análisis de la Sentencia No. 839-14-Ep/21 de la Corte Constitucional del Ecuador menciono que;

> En el caso 839-14-EP, la Corte Constitucional emitió una sentencia donde se resolvió una acción de acceso a la información pública presentada por un ciudadano contra el SRI, solicitando acceder a la declaración de impuesto a la herencia de su hermana. La demanda fue aceptada en primera y segunda instancia, ya que se consideró que la autoridad pública no había justificado la reserva de la información solicitada y que el solicitante cumplió con los requisitos para acceder a la misma. Ante esto, el SRI interpuso una acción extraordinaria de protección contra la decisión de segunda instancia (p.3).

4. Objetivo general

Analizar la aplicación de la responsabilidad civil y penal, así como el régimen sancionatorio por incumplimiento de la cláusula de protección de datos en el Servicio de Rentas Internas de Ecuador, con el fin de fortalecer la seguridad jurídica y la protección efectiva de los derechos personales en el ámbito tributario.

4.1. Objetivo especifico

1. Desarrollar de manera teórica-doctrinaria la protección de datos personales y sus aspectos más relevantes dentro de la normativa ecuatoriana.
2. Analizar las medidas implementadas por el Servicio de Rentas Internas en relación con la protección de datos personales, evaluando su eficacia y adecuación a lo establecido por la Constitución ecuatoriana y la Ley de Protección de Datos Personales y su reglamento.
3. Identificar posibles deficiencias, debilidades y áreas de mejora en el cumplimiento normativo y la gestión de riesgos en materia de protección de datos por parte del Servicio de Rentas Internas, con el objetivo de proponer recomendaciones para fortalecer el régimen sancionatorio y la protección de datos.

5. Justificación y aplicación metodológica

5.1. Justificación

En el contexto ecuatoriano, a pesar de contar con disposiciones constitucionales y una Ley de Protección de Datos y su reglamento recientemente vigente, se identifica una carencia significativa en cuanto a las sanciones por el incumplimiento de estas normas, especialmente en entidades como el Servicio de Rentas Internas. No obstante, a pesar de la existencia de normativa, se observa una falta significativa en cuanto a la definición y aplicación de sanciones civiles y penales por el incumplimiento de las disposiciones de protección de datos en una entidad pública crucial como el Servicio de Rentas Internas.

La presente investigación se propone abordar esta problemática desde una perspectiva jurídica, con el objetivo de analizar cómo se lleva a cabo la asignación de responsabilidades civiles y penales, así como el establecimiento y aplicación de sanciones en casos de incumplimiento de las regulaciones de protección de datos en el Servicio de Rentas Internas de Ecuador. Se trata de examinar en profundidad la naturaleza de las medidas implementadas hasta la fecha por esta entidad en lo que respecta a la protección de datos personales, evaluando su eficacia y conformidad con lo dispuesto por la normativa nacional e internacional en esta materia.

La relevancia de esta investigación radica en la necesidad apremiante de garantizar la protección efectiva de los derechos personales en el ámbito tributario ecuatoriano, promoviendo la transparencia, la seguridad jurídica y el cumplimiento de principios constitucionales fundamentales en materia de privacidad y protección de datos. En un contexto donde la información personal es un activo valioso y vulnerable a la vez, resulta imperativo establecer mecanismos sólidos para prevenir y sancionar el uso indebido de dicha información, especialmente cuando proviene de entidades públicas con un acceso significativo a datos sensibles de los ciudadanos.

A través de un análisis minucioso de las prácticas y políticas implementadas por el Servicio de Rentas Internas en relación con la protección de datos, esta investigación pretende otorgar un aporte académico al identificar posibles deficiencias, debilidades y áreas de mejora en el ámbito del cumplimiento normativo y la gestión de riesgos en materia de privacidad. Asimismo, se

propone evaluar la coherencia y efectividad de las medidas adoptadas por esta entidad para garantizar la confidencialidad y seguridad de la información personal que maneja, considerando las implicancias legales, éticas y prácticas de su accionar en este sentido.

La necesidad de la presente investigación radica en identificar hallazgos y conclusiones que puedan contribuir a la optimización del régimen sancionatorio aplicable en casos de incumplimiento de la normativa de protección de datos en el ámbito tributario, fortaleciendo la capacidad del Estado para proteger los derechos fundamentales de los individuos frente a posibles abusos o vulneraciones de su privacidad. Asimismo, se busca fomentar una cultura de respeto y responsabilidad en el tratamiento de la información personal dentro de las instituciones públicas, promoviendo la transparencia, la rendición de cuentas y la salvaguarda de la intimidad de los ciudadanos en el entorno digital actual.

5.2. Metodología

Nivel de estudio

En este estudio se analizará la cláusula de protección de datos personales presente en el acuerdo de uso de medios electrónicos del Servicio de Rentas Internas (SRI) en Ecuador. Se examinarán aspectos legales y técnicos relativos a la protección de datos en el entorno digital del país y las sanciones en cuanto al incumplimiento de la cláusula.

Modalidad de la investigación

Para abordar este problema desde un enfoque cualitativo, es importante realizar investigación de campo, entrevistas con funcionarios del SRI, expertos en protección de datos personales y abogados especializados en la materia. Además, se utilizará el análisis documental, revisando la normativa vigente, informes de organismos internacionales, jurisprudencia relacionada, entre otros documentos relevantes. Es fundamental que la investigación cualitativa se base en un marco teórico sólido y se realice un análisis profundo y detallado de los datos recopilados, buscando identificar patrones, tendencias y posibles soluciones al problema planteado.

5.3. Métodos

El método inductivo es apropiado para abordar este problema, ya que implica la observación de casos específicos para llegar a conclusiones generales. En este caso, se pueden analizar casos concretos de incumplimiento de la normativa en protección de datos en el SRI, así como las respuestas y medidas tomadas por la institución en cada caso. A partir de esta observación, se pueden identificar patrones y tendencias que permitan comprender mejor la aplicación de la responsabilidad civil y penal en este contexto.

CAPITULO 1: LOS DATOS PERSONALES

1.1. Conceptualización

> Los datos representan información organizada para ser manejada por un ordenador o una persona. Es cualquier dato relacionado con una persona viva que pueda identificarla directa o indirectamente. Aunque se haya eliminado la identificación de los datos personales mediante cifrado o seudonimización[1] (Contreras, 2020).

Es decir que, es cualquier información relacionada con una persona física identificada o identificable (el interesado). Una persona se considera identificable cuando su identidad puede determinarse, ya sea de manera directa o indirecta, especialmente mediante un identificador como un nombre, número de identificación, datos de localización, identificador en línea, o varios rasgos característicos de su identidad física, fisiológica, genética, psicológica, económica, cultural o social (Rivera, 2023). Por lo tanto, cualquier información relacionada o que pueda ser vinculada a una o más personas naturales identificadas o identificables, tales como nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información asociada a la identidad del titular es un dato personal.

[1] Agencia española de protección de datos (2021) “implica el reemplazo de información que identifica directamente a una persona” (p.23).

Desde una perspectiva doctrinal, los datos personales se pueden dividir en dos categorías principales: datos personales públicos y datos personales privados. Los datos públicos son aquellos que pueden ser accesibles por terceros debido a su naturaleza pública (Martínez, et. al, 2023, p.12). Por ejemplo, la información disponible en sitios públicos, directorios profesionales, guías telefónicas e incluso en redes sociales se incluye en esta categoría.

Los datos personales privados comprenden información íntima del individuo, y pueden clasificarse en diferentes grados según su naturaleza. (Contreras, 2020) explica estos grados de la siguiente manera:

- Datos personales, como los tributarios, censales o catastrales, aunque protegidos por la ley, pueden ser divulgados bajo ciertas normativas legales, especialmente en el marco de procedimientos judiciales o administrativos.
- Datos secretos, referidos a aspectos como la raza, la salud o la vida sexual, no deben ser revelados salvo en casos específicos permitidos por la ley.
- Datos profundos, relacionados con la ideología, creencias religiosas u opiniones políticas, deben mantenerse en el ámbito privado de la persona sin excepción (Contreras, 2020).

1.2. La protección de datos personales en el Derecho internacional

La ONU, la OEA y la Comisión Europea han liderado la creación de leyes sobre datos personales. De acuerdo con la Comisión Europea, los datos personales se definen como información sobre una persona viva que puede identificarse. La recopilación de diferentes datos que juntos pueden identificar a una persona también se considera datos personales (Contreras, 2020).

Según la Organización de Estados Americanos (OEA), los datos personales son aquella información que, de forma directa o indirecta, permite identificar a una persona específica, ya sea mediante un número de identificación o a través de varios factores relacionados con su identidad física, fisiológica, mental, económica, cultural o social (González, 2007). Por otro lado, esta definición no

incluye la información que no permite identificar o no se puede utilizar para identificar a una persona en particular.

Igualmente, la Comisión Europea ha definido cuáles son considerados datos personales y cuáles no lo son. En primer lugar, se consideran datos personales el nombre y apellidos, dirección, correo electrónico, DNI, datos de localización (como la ubicación de un teléfono móvil), dirección IP, identificador de cookie, identificador de publicidad en el teléfono y datos médicos que puedan identificar única e inequívocamente a una persona (González, 2007).

Por consiguiente, no se pueden considerar como datos personales los números de registro mercantil, direcciones de correo electrónico o datos anonimizados[2], como establece la Comisión Europea en el año 2021. Este organismo ha sido pionero en la protección de la privacidad de los datos al promulgar la Ley de Protección de Datos en 2016 y el Reglamento General de Protección de Datos en 2021 (González, 2007).

Dentro de los derechos fundamentales protegidos por el RGPD se encuentran el derecho al olvido, a la portabilidad y al acceso. Las normas para la protección y privacidad de los datos personales, según los Principios de la OEA, buscan garantizar que las personas reciban información pertinente sobre quién recopila sus datos, con qué propósito, qué medidas de protección existen y cómo pueden ejercer sus derechos. Se debe asegurar que aquellos que manejan datos personales lo hagan de manera adecuada, respetando los derechos de la persona.

La Red Iberoamericana de Protección de Datos Personales ha elaborado un documento titulado Estándares de Protección de Datos Personales para los Estados Iberoamericanos, con el objetivo de afirmar que la seguridad de los datos personales es fundamental para salvaguardar otros derechos. Este texto establece una serie de principios que rigen el tratamiento de los datos personales, como la legitimidad, legalidad, transparencia, finalidad,

[2] Agencia española de protección de datos (2021) “datos personales que se han procesado de manera que ya no pueden ser asociados a una persona específica sin información adicional que esté separada y resguardada de manera segura” (P.22)

proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad, así como los derechos del titular de los datos.

1.3. Reglamento General de Protección de datos personales mayor estándar de protección

El Reglamento General de Protección de Datos es, indudablemente, la normativa legal más relevante en términos de protección de la privacidad y seguridad de la información. Es considerado el instrumento jurídico más impactante en la historia, transformando la forma en que se manejan los datos personales a nivel mundial. Basado en la gestión de riesgos, ha revolucionado el procesamiento de datos. Las multas pueden llegar al 4% de la facturación anual de una entidad, ya sea pública o privada (Roca, 2020). A pesar de ello, aún existen muchas dudas sobre cómo cumplir con sus requerimientos.

El Reglamento General de Protección de Datos es una normativa implementada por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea con el propósito de fortalecer y armonizar la protección de datos para todos los residentes de la Unión Europea (UE). Además, aborda la transferencia de datos personales fuera de la UE. El objetivo principal del GDPR es ofrecer a los ciudadanos y residentes mayor control sobre sus datos personales y facilitar el entorno regulatorio para las empresas internacionales mediante una normativa unificada en toda la UE.

El Reglamento General de Protección de Datos establece normas estrictas para el tratamiento de información personal que se basan en el consentimiento del individuo. Estas normas buscan asegurar que las personas entiendan claramente qué están consintiendo. Por lo tanto, el consentimiento debe ser dado de forma libre, específica, informada e inequívoca, a través de una solicitud presentada en un lenguaje claro y sencillo. Este consentimiento se debe expresar mediante un acto afirmativo, como marcar una casilla en línea o firmar un documento.

Cuando una persona otorga su consentimiento para el tratamiento de sus datos personales, estos solo podrán ser utilizados para los fines específicos para los cuales dio su aprobación. Además, debe tener la opción de retirar su

consentimiento en cualquier momento. Las personas deben recibir información clara sobre quién está tratando sus datos y por qué (Blanco, 2018). Como mínimo, deberían conocer lo siguiente:

- La identidad del responsable del tratamiento
- Los motivos por los cuales se están tratando sus datos personales
- La base legal para dicho tratamiento
- Quiénes recibirán los datos (si corresponde) (Macén, 2021).

En ciertos casos, la información proporcionada también debe incluir:

- Los datos de contacto del delegado de protección de datos (si es aplicable)
- Los intereses legítimos de la empresa si se justifican con esta base legal para el tratamiento
- Las medidas adoptadas para transferir los datos a un país fuera de la UE
- El periodo durante el cual se almacenarán los datos
- Los derechos del individuo en materia de protección de datos (como acceso, rectificación, supresión, limitación, oposición, portabilidad, etc.)
- El derecho a retirar el consentimiento (cuando éste sea la base legal para el tratamiento)
- Si la entrega de datos es un requisito legal o contractual
- En caso de decisiones automatizadas, información sobre la lógica aplicada, la importancia y las consecuencias de la decisión (Macén, 2021).

Toda esta información debe ser presentada de manera clara y sencilla para que sea fácilmente entendible por cualquier individuo.

Si una persona considera que sus datos personales son incorrectos, incompletos o inexactos, tiene el derecho de rectificarlos o completarlos sin demoras indebidas. En tal caso, es necesario informar a todos los destinatarios de esos datos sobre cualquier modificación o eliminación realizada. Si los datos compartidos son incorrectos, también puede ser necesario notificar a todas las

personas que los hayan consultado previamente (a menos que esto implique un esfuerzo desproporcionado).

> Una persona también tiene el derecho de oponerse en cualquier momento al tratamiento de sus datos personales para un uso específico si la empresa los gestiona con base en un interés legítimo o para actividades de interés público. En esta situación, la empresa debe cesar el tratamiento de los datos personales a menos que el interés legítimo de la empresa supere el del individuo (Martínez R. , 2017).

Asimismo, una persona puede solicitar la limitación del tratamiento de sus datos personales mientras se determina si el interés legítimo de la empresa prevalece sobre su interés individual. Sin embargo, en el caso de fines comerciales directos, la empresa siempre debe cesar el tratamiento de los datos personales si así lo solicita el interesado.

Este reglamento no solo cambia la forma en que se protegen los datos personales a nivel mundial, sino que también afecta significativamente a la industria de la ciberseguridad al basarse en la gestión de riesgos. Con un alcance global, todas las organizaciones, públicas y privadas, que manejen datos de forma automatizada deben cumplir con sus disposiciones. Varios países en Latinoamérica y algunos estados de EE. UU. han optado por seguir el camino marcado por el Reglamento, lo que está llevando a una reforma de las leyes de protección de datos en todo el mundo para ajustarse a esta normativa europea

1.4. Los datos personales en la normativa de América Latina

La Ley 25326 de Argentina, que fue la primera normativa de protección de datos en América Latina y que se basó en el modelo de la directiva europea 95/46/CE, está actualmente en proceso de revisión debido a su obsolescencia, especialmente en comparación con el nuevo estándar internacional establecido por el Reglamento General de Protección de Datos de la Unión Europea (GDPR).

La ley peruana de protección de datos ha sido efectiva en términos de derechos, principios y consecuencias, pero es anterior a la entrada en vigor del GDPR, por lo que se prevé una reforma. Esta también fue la primera normativa de protección de datos de la Comunidad Andina de Naciones. De manera similar, la ley

colombiana de protección de datos sigue el modelo de la Directiva (UE) 95/46/CE, por lo que también requiere una actualización de acuerdo con el GDPR (González, 2007).

CAPITULO 2: El Derecho a la Protección de datos

2.1. Definición

La protección de datos se refiere a los derechos de las personas cuya información se recopila, se mantiene y se procesa, para saber qué información se retiene y se utiliza, y para corregir posibles inexactitudes. En la investigación, es importante considerar las obligaciones legales y éticas en cuanto a compartir los datos de acuerdo con la Ley de Protección de Datos de 1998 en el Reino Unido (Córdoba, et.al, 2020).

Es crucial tener en cuenta conceptos como el controlador de datos, que es la persona u organización que determina cómo se procesan los datos personales, y los datos personales que se refieren a la información que puede revelar la identidad de una persona viva.

Por otro lado, (Roca, 2020) menciona que, el derecho a la protección de datos garantiza nuestra capacidad de controlar y disponer de nuestros propios datos personales, señala además que;

> Este derecho es protegido a nivel nacional, comunitario e internacional, y su objetivo principal es asegurar la protección de nuestros datos. El derecho fundamental a la protección de datos está reconocido y protegido en varios ámbitos, siendo especialmente relevantes el artículo 18.4 de la Constitución, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (p. 168).

2.2. Principios del derecho a la protección de datos personales

Los principios de protección de datos personales son fundamentales para salvaguardar la privacidad y seguridad de la información en la era digital. Estos principios, que incluyen la legalidad, transparencia, minimización de datos, exactitud, integridad, y confidencialidad de la información, aseguran que los

datos personales sean tratados de acuerdo con marcos legales estrictos y criterios éticos. Implementarlos no solo protege a los individuos de posibles abusos y vulneraciones, sino que también fortalece la confianza entre usuarios y organizaciones.

La adhesión a estos principios permite un manejo responsable y seguro de la información, promoviendo un balance entre innovación tecnológica y derechos fundamentales del ser humano**.** Según manifiesta (Roca, 2020), existen varios principios que derivan de la protección de datos personales:

- **Principio de limitación en la recolección de los datos**: implica que la recopilación de información debe ser adecuada, relevante y limitada a lo estrictamente necesario para los fines previstos. Este principio se basa en que los datos personales deben ser pertinentes y utilizados solo para los propósitos específicos para los que se recopilan, garantizando que no se recopilen más datos de los necesarios y que se utilicen únicamente para los fines establecidos.
- **Principio de calidad de los datos:** La información personal debe ser pertinente para su uso previsto y mantenerse precisa, completa y actualizada en la medida necesaria para dicho fin.
- **Principio de especificación del propósito:** La finalidad de la obtención de datos debe ser claramente indicada en el momento de la recopilación, y su uso se limitará a cumplir con los objetivos originales o con otros fines que no sean incompatibles, especificando cualquier cambio de objetivo en cada caso.
- **Principio de limitación de uso:** No se deben compartir, hacer accesibles ni utilizar los datos personales para fines que no cumplan con lo establecido en el principio anterior, a menos que se cuente con el consentimiento del individuo involucrado, o que sea requerido por ley o por autoridades competentes (por ejemplo, que los datos recolectados para decisiones administrativas puedan ser utilizados para investigaciones, estadísticas y planificación social).
- **Principio de salvaguardia de la seguridad:** Se implementarán medidas de seguridad adecuadas para proteger la información personal de posibles riesgos como pérdida, acceso no autorizado, destrucción,

modificaciones o divulgación. Es importante tener en cuenta que la seguridad y la privacidad no son lo mismo. Las restricciones en el uso y la divulgación de los datos deben estar respaldadas por medidas de seguridad tales como medidas físicas.

- **Principio de transparencia:** Es necesario establecer una política de transparencia que abarque la evolución, prácticas y normativas relacionadas con los datos personales. Se deben contar con mecanismos rápidos para identificar la presencia y la naturaleza de los datos personales, el propósito principal de su uso, así como la identidad y la ubicación habitual del responsable de dichos datos.
- **Principio de participación individual:** Cada persona tiene el derecho de confirmar si una fuente tiene datos sobre ellos, solicitar que se les comuniquen los datos relacionados con su persona en un plazo razonable y a un costo razonable, de manera clara y comprensible. También tienen derecho a que se les expliquen las razones detrás de una negativa a su solicitud y a cuestionar dicha negativa. Además, pueden expresar dudas sobre los datos relacionados con ellos mismos y, si su reclamación tiene éxito, lograr que se eliminen, rectifiquen, completen o corrijan dichos datos.
- **Principio de responsabilidad:** Es responsabilidad principal del controlador de datos garantizar que se cumplan las medidas que aseguren el cumplimiento de los principios mencionados anteriormente (Roca, 2020).

Por otro lado, en el ámbito ecuatoriano la (Ley Orgánica de Protección de datos personales, 2021) establece una serie de principios:

- **Juridicidad. -**Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la norma.
- **Lealtad.** -El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán

tratados. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.

- **Transparencia. -**El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.
- **Finalidad. -** Las razones para tratar los datos deben ser claras, específicas, legítimas y comunicadas al propietario de los datos. No se podrán usar los datos personales para propósitos distintos a aquellos para los cuales fueron recopilados.
- **Pertinencia y minimización de datos personales. -** Los datos personales deben ser relevantes y limitados a lo estrictamente necesario para cumplir con la finalidad del tratamiento de datos.
- **Proporcionalidad del tratamiento. -** El tratamiento de datos debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación con las finalidades para las cuales fueron recopilados o con la naturaleza de las categorías especiales de datos.
- **Confidencialidad. -** El tratamiento de datos personales debe basarse en el sigilo y secreto adecuados, evitando su uso o comunicación para fines distintos a los originalmente previstos.
- **Calidad y exactitud. -** Los datos personales que se procesen deben ser exactos, completos, precisos, íntegros, verificables y claros; y, si es necesario, actualizados correctamente para mantener su veracidad.
- **Conservación. -** Los datos personales se conservarán solo durante el tiempo estrictamente necesario para cumplir con la finalidad para la que se tratan.
- **Seguridad de datos personales. -** Los responsables y encargados del tratamiento de datos personales deben implementar todas las medidas de seguridad necesarias y adecuadas.
- **Responsabilidad proactiva y demostrada. -** El responsable del tratamiento de datos personales debe demostrar que ha implementado mecanismos para proteger estos datos, cumpliendo con los principios, derechos y obligaciones establecidos en la Ley.

- **Aplicación favorable al titular. -** En caso de dudas sobre el alcance de las disposiciones legales o contractuales aplicables a la protección de datos personales, los funcionarios judiciales y administrativos interpretarán y aplicarán dichas disposiciones en el sentido más favorable para el titular de los datos.
- **Independencia del control. -** Para asegurar el ejercicio efectivo del derecho a la protección de datos personales y cumplir con las obligaciones del Estado debe ejercer un control independiente, imparcial y autónomo, y realizar acciones de prevención, investigación y sanción según corresponda (Ley Orgánica de Protección de datos personales, 2021).

2.3. Protección de datos en Ecuador

Desde el punto de vista normativo, los datos personales se refieren a cualquier información que pueda utilizarse para identificar a una persona viva, ya sea de forma directa o indirecta. No hay una lista definitiva que establezca qué constituye datos personales, ya que esto puede variar según el contexto en el que se utilice la información. La recolección, procesamiento y almacenamiento de datos personales están estrictamente regulados por normativas como el Reglamento General de Protección de Datos en Europa, y es importante tratar estos datos con precaución, especialmente aquellos que contienen información sensible que pueda exponer a las personas a discriminación o a riesgos significativos (González, 2007).

La Constitución de la República del Ecuador consagra principios fundamentales que definen la estructura y los valores del Estado. En su artículo 1, se establece que Ecuador es un Estado constitucional que prioriza los derechos y la justicia, con un carácter social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Esta definición subraya un compromiso firme con la inclusión y la diversidad cultural, así como con la independencia y la soberanía nacional.

Además, la Constitución de 2008, en su artículo 3, detalla claramente las obligaciones del Estado hacia sus ciudadanos. Entre estas obligaciones, se destaca la garantía del disfrute pleno y sin discriminación de los derechos

humanos. Esto incluye un amplio espectro de derechos consagrados en la normativa nacional e internacional que Ecuador ha adoptado y firmado. Este compromiso con los derechos humanos y la justicia social representa un pilar fundamental en la gobernanza ecuatoriana, asegurando que ninguna persona sea excluida o discriminada en el ejercicio de sus derechos.

El Artículo 11 de la Constitución de la República del Ecuador (2008) establece un marco claro para el ejercicio y la protección de los derechos fundamentales. En primer lugar, estipula que los derechos pueden ser ejercidos tanto de manera individual como colectiva ante las autoridades competentes, quienes tienen la obligación de garantizar su cumplimiento. La igualdad de derechos, deberes y oportunidades para todas las personas es un principio fundamental, asegurando así que no haya discriminación en la base del espectro de derechos reconocidos por el Estado.

Además, el artículo enfatiza que los derechos y garantías consignados en la Constitución, así como en los instrumentos internacionales de derechos humanos, tienen aplicación directa e inmediata. Esto significa que todos los servidores públicos están obligados a aplicarlos en el ejercicio de sus funciones, ya sea de oficio o a solicitud de parte interesada. Este enfoque asegura que la protección y promoción de los derechos humanos sea una prioridad constante y operativa en todas las esferas del gobierno y la administración pública.

En esencia, el Artículo 11 refuerza el compromiso del Estado ecuatoriano con un sistema de derechos humanos integral y efectivo, donde cada persona puede exigir el respeto y cumplimiento de sus derechos en igualdad de condiciones, y donde los servidores públicos actúan como garantes proactivos de estos derechos.

Por otro lado, el Artículo 16 Derecho a la Comunicación, todas las personas, individual y colectivamente, tienen el derecho fundamental a una comunicación libre, diversa, inclusiva, intercultural y participativa en todas las esferas de la interacción social. Este derecho abarca la capacidad de expresarse y recibir información por cualquier medio y forma, en su idioma y utilizando sus propios símbolos y formas de expresión cultural.

El Estado garantiza el acceso universal a las tecnologías de información y comunicación, asegurando que estas herramientas estén disponibles para todos, sin discriminación alguna. Además, se promueve un entorno en el que la pluralidad de voces y culturas pueda coexistir y enriquecerse mutuamente, fomentando una sociedad más equitativa y con respeto a la diversidad.

Por consiguiente, la protección de datos según la Constitución de la República del Ecuador (2008), reconoce y garantiza el derecho de toda persona a la privacidad y a la protección de su información personal. Este derecho se fundamenta en los siguientes principios:

- Autorización del Titular. - La recolección, almacenamiento, procesamiento y distribución de información personal requiere el consentimiento explícito del titular de los datos, salvo disposición legal que indique lo contrario.
- Control sobre Datos Personales. - El titular tiene el derecho de acceder, rectificar, actualizar y eliminar su información personal de cualquier base de datos (Rivera, 2023).

El marco constitucional también protege el derecho a la intimidad personal y familiar, lo cual incluye varios aspectos clave:

- Inviolabilidad de la Correspondencia. - La correspondencia, ya sea física o virtual, es inviolable. El Estado y terceros están obligados a respetar este derecho.
- Secreto de la Comunicación. - La Constitución establece que todas las formas de comunicación deben mantenerse en secreto, siendo prohibida su inspección, salvo en casos excepcionales previstos por la ley y con la debida autorización judicial (Sanmartín, 2022).

El Estado ecuatoriano tiene la responsabilidad de garantizar y proteger los derechos relacionados con la privacidad y la protección de los datos personales mediante:

- Legislación Adecuada. - Creación y mantenimiento de un marco legal que resguarde esos derechos.

- Interpretación Judicial. - La intervención en materia de privacidad solo será permitida bajo circunstancias excepcionales y con la debida orden de autoridad judicial competente.
- Protección y Seguridad de Datos. - Implementación de medidas necesarias para proteger la información personal de accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas (Valdiviezo, 2021).

Según el numeral 19 del artículo 66 de la Constitución de la República del Ecuador (2008), el derecho a la protección de datos personales es esencial para la libertad individual. Este derecho garantiza a cada persona el control sobre su información personal, permitiéndole acceder, decidir sobre su uso y proteger sus datos frente a posibles abusos o mal uso por parte de terceros.

Por otro lado, el artículo 92 de la misma Constitución consagra la Acción de Habeas Data como una herramienta legal que asegura a los ciudadanos el derecho a conocer, acceder y, de ser necesario, rectificar los datos personales contenidos en bancos, archivos o documentos que les conciernan. Esta acción ampara no solo el acceso a la información, sino también garantiza la transparencia sobre su origen, utilización, finalidad, destino y vigencia, brindando un marco de protección robusto para los datos personales y reforzando la seguridad y confianza en la gestión y uso de la información personal.

En suma, la Constitución del Ecuador establece un marco constitucional sólido que tutela tanto el acceso como la protección integral de los datos personales de sus ciudadanos, promoviendo un equilibrio entre la libertad individual y la responsabilidad en el manejo de la información personal.

Las personas responsables de estos datos deben asegurar que cualquier divulgación de la información cuente con la autorización del titular o cumpla con los requisitos legales vigentes. El titular de la información tiene el derecho de solicitar acceso gratuito a su archivo, así como actualizar, corregir, eliminar sus datos o pedir su anulación. En el caso específico de datos sensibles, es imprescindible que su conservación esté debidamente autorizada por la ley o el

titular, y que se implementen rigurosas medidas de seguridad para proteger dicha información.

Si la solicitud del titular no es atendida, la persona afectada tiene el derecho de recurrir a un juez para buscar una resolución y demandar la compensación por los perjuicios ocasionados. Este mecanismo asegura que el procesamiento de datos personales se realice con respeto a los derechos y la privacidad de los individuos.

El 14 de diciembre marca un hito importante en la protección de la privacidad a nivel global, con la adopción de la resolución 45/95 por parte de la ONU, que establece normativas para la regulación de los espacios de almacenamiento de datos personales, junto con garantías mínimas que deben ser aplicadas en las legislaciones nacionales. En este contexto, Ecuador ha mostrado su compromiso con la protección de datos personales al participar como Estado observador en la Red Iberoamericana de Protección de Datos (Vivar, et.al, 2020). Esta participación culminó en la aprobación de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, durante el XV Encuentro Iberoamericano de Protección de Datos Personales celebrado en junio de 2017, destacando así su compromiso con la adopción de las mejores prácticas en esta materia.

El 27 de marzo de 2015, la Organización de Estados Americanos (OEA) presentó una propuesta pionera de legislación modelo para la protección de datos personales. Esta iniciativa refleja la creciente importancia de resguardar la información personal en el entorno digital, esencial para el desarrollo de la sociedad de la información y el conocimiento. Según se detalla en el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018, garantizar la protección de los datos personales es un pilar fundamental para construir una sociedad donde la comunicación y el conocimiento son motores del progreso (Vivar, et al., 2020, p.12).

En este contexto, Ecuador, como miembro activo de la comunidad internacional y participante en la sociedad digital global, debe adherirse a estas directrices de la OEA. La implementación de unas robustas políticas de protección de datos no

solo asegura la privacidad de los ciudadanos ecuatorianos, sino que también fortalece la confianza en el uso de plataformas digitales y promoción del comercio electrónico. Además, al alinearse con las normativas internacionales, Ecuador puede mejorar su competitividad y colaborar de manera más eficaz en iniciativas regionales e internacionales.

CAPITULO 3: Derechos ARCOS

3.1. Definición

“La denominación derechos ARCO proviene de un acrónimo que representa los cuatro derechos principales reconocidos en la legislación de protección de datos personales en varios países, como México y Argentina. Estos derechos son: acceso, rectificación, cancelación y oposición” (Benoit, 2022, p. 399). Esta sigla sintetiza las facultades otorgadas a los titulares de los datos personales para que puedan controlar cómo se manejan sus datos en sistemas de información tanto públicos como privados. Es importante destacar que estos derechos no son los únicos; existen muchas otras facultades que corresponden a los interesados, como la adición, actualización, confidencialidad y disociación de los datos, entre otras.

> Los derechos ARCO se refieren a un conjunto de facultades diseñadas para proteger al máximo los datos personales, permitiendo que cada individuo mantenga el control sobre el registro, uso y relevancia de sus datos. En la mayoría de los países que han integrado la protección de datos personales en sus sistemas legales, se han adoptado estas facultades para beneficio del titular de los datos. Los derechos ARCO, que incluyen acceso, rectificación, cancelación y oposición (Luna, 2019).

Según (Bettoch, 2018) los Derechos ARCO está compuesto por los siguientes Derechos:

- **El Derecho al acceso:** El derecho de acceso permite a una persona dirigirse al responsable o encargado de un archivo o tratamiento de datos para conocer todos los datos personales que le conciernen. Además, la persona puede recibir una copia comprensible de dichos datos y obtener

información sobre su origen. Al ejercer este derecho, la persona puede informarse sobre las finalidades del tratamiento, el tipo de datos registrados, su origen, los destinatarios de los datos y las posibles transferencias de datos a otros países.

- **Derecho de rectificación:** Es el derecho de una persona a solicitar al responsable de un fichero o tratamiento de datos que corrija sus datos personales. La petición de corrección debe especificar el dato que se considera incorrecto y la modificación que se debe hacer, además de estar acompañada de la documentación que respalde la solicitud de corrección.
- **Derecho de cancelación:** Este derecho permite a las personas solicitar al responsable de los datos que elimine su información personal.
- **Derecho de oposición:** Cada individuo tiene el derecho de rechazar la recolección de sus datos personales, su entrega a terceros o su transferencia. Esto sucede cuando la persona objeta alguna de estas acciones y su interés particular, debido a su situación específica, tiene mayor peso que el interés del encargado del banco de datos (Bettoch, 2018).

3.2. Bases legitimas

El artículo 92 de la Constitución de la República del Ecuador (2008), en el Capítulo de Garantías Jurisdiccionales, se refiere al habeas data. Establece que toda persona, ya sea por su propio derecho o en calidad de representante autorizado, tiene el derecho de acceder y conocer la existencia de documentos, datos genéticos, bases de datos personales y archivos que contengan información sobre sí misma o sobre sus bienes, ya sea en formato físico o electrónico. También tiene el derecho de saber cómo se utilizan esos datos, su propósito, el origen y destino de la información personal, así como el tiempo durante el cual se mantendrá en el archivo o base de datos.

Las personas encargadas de administrar bancos o archivos de datos personales podrán divulgar la información almacenada solo si tienen la autorización del titular de los datos o si la ley así lo permite. La persona propietaria de los datos tiene el derecho de solicitar al encargado acceso gratuito a su información, así

como la actualización, corrección, eliminación o anulación de sus datos. Cuando se trate de datos sensibles, cuyo almacenamiento requiere estar autorizado por la ley o por la misma persona propietaria, deberán implementarse las medidas de seguridad necesarias. Si la solicitud no es atendida, el titular podrá recurrir a un juez o jueza. La persona afectada también tiene el derecho de reclamar por los daños ocasionados.

Del texto del precepto se derivan varias dimensiones que protege la Acción de habeas data: el derecho a saber de la existencia y acceder a los documentos, datos genéticos, y archivos de datos personales, así como informes que estén en poder de entidades públicas o privadas, sin importar cómo se tratan esos datos. Además, se tiene el derecho a conocer el uso, propósito, origen y destino de sus datos; y el derecho a actualizar, rectificar, eliminar o anular dichos datos.

Es esencial destacar dos conceptos presentes en las normativas sobre protección de datos. El primero es el de finalidad, que se refiere al objetivo del tratamiento de los datos, orientado a cumplir con ciertas expectativas de los bancos o archivos de datos personales. En segundo lugar, es importante señalar que los derechos relativos a los datos personales se ejercen independientemente de cómo se traten dichos datos, del tipo de soporte en el que se encuentren o de si la entidad que los posee es pública o privada.

Del texto constitucional se puede inferir la creación de una categoría específica de datos sensibles, a los cuales se deben aplicar medidas de seguridad adecuadas para garantizar su protección, integridad y privacidad. Estos datos se refieren a cualquier información relacionada con personas físicas que puedan ser identificadas o identificables. La acción de habeas data surge como un mecanismo para que las personas puedan proteger su derecho al honor, la privacidad y asegurarse de que la información recopilada sobre ellas sea precisa, pertinente, actualizada y confiable, y que no se utilice para fines distintos a los que fue recogida.

El derecho a acceder a los documentos, bancos de datos e informes relacionados con el interesado o sus bienes, que se encuentren en entidades públicas o privadas, permite al propio interesado, siempre que lo acredite

adecuadamente, conocer la información que estas entidades están gestionando sobre él, independientemente de la forma de tratamiento o los medios empleados. Este acceso incluye información sobre el propósito para el cual los datos fueron incorporados al banco de datos y el uso que se les está dando, las posibles transferencias de información que se hayan realizado, así como la identidad y dirección del responsable del banco de datos o fichero. El responsable debe facilitar este acceso sin ningún costo para el ciudadano, garantizando así la gratuidad del mismo.

En segundo lugar, se establece el derecho a que los datos sean actualizados o corregidos en caso de inexactitud, distorsión, falsedad o error, asegurando que la información registrada sobre los ciudadanos sea precisa y acorde a la realidad actual. Finalmente, se reconoce el derecho de las personas a que sus datos sean eliminados o anulados si son incorrectos, si la finalidad para la que fueron recopilados ha finalizado sin que haya una normativa que justifique su conservación, o si afectan de manera ilegítima los derechos de las personas.

CAPITULO 4: DISCUSIÓN TEÓRICA DOCTRINARIA

4.1. La protección de datos personales

Generalidades

A nivel global, se está tomando conciencia de la importancia de establecer un marco legal para proteger y manejar adecuadamente los datos personales. En mayo de 2016, el Consejo de Europa aprobó el Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2018. El propósito principal de esta normativa es fortalecer la protección de datos y actualizar las directrices anteriores que no abordaban los nuevos desafíos tecnológicos.

> El RGPD ha establecido un nuevo estándar que se considera como punto de referencia para futuras legislaciones que busquen desarrollar normas específicas de protección de datos. En América Latina, Brasil ha decidido mejorar sus medidas de protección de datos para cumplir con los requerimientos del RGPD (Contreras, 2020).

Existen razones económicas que incentivan a los Estados a implementar leyes de protección de datos adecuadas. Por ejemplo, tener un marco legal sólido puede atraer inversiones internacionales y actividades empresariales que involucran la transferencia de datos personales, lo que podría mejorar la competitividad en el sector de las TIC. Un marco normativo completo y actualizado en materia de protección de datos fomenta la confianza y la seguridad jurídica en el uso de los datos, lo que a su vez impulsa la economía y la innovación en la sociedad de la información.

La relación entre el derecho a la intimidad y el derecho a la protección de datos personales, también conocido como autodeterminación informativa, ha sido ampliamente estudiada por diferentes corrientes doctrinales, normativas y jurisprudenciales. En términos generales, se reconoce la importancia de proteger los datos de las personas para que sean utilizados de manera adecuada y solo con el consentimiento correspondiente. La protección de datos se define como la parte de la legislación que resguarda la libertad individual y el derecho a la intimidad en relación al tratamiento de información personal, ya sea de forma manual o automática. En la normativa europea, se considera como datos personales a toda información que identifique o pueda identificar a una persona física (Proaño, 2021).

Debido al impacto de las nuevas tecnologías en la recolección, procesamiento y transmisión de datos personales, resulta necesario abordar el tema de la protección de datos desde sus desafíos iniciales. En el contexto de la sociedad digital, el concepto de intimidad confiere derechos a los individuos sobre sus datos personales sujetos a tratamiento automatizado, así como impone obligaciones a quienes controlan y acceden a los archivos.

Es importante destacar que la protección de la veracidad de los datos y su uso no se limita exclusivamente a la intimidad, sino que el derecho a la protección de datos abarca también los intereses colectivos frente al procesamiento y almacenamiento de información. Siguiendo la idea de la tercera generación de derechos, la sociedad tecnológica ha dado lugar a la figura del "hombre artificial", cuya existencia se define en un entorno artificial generado por la propia humanidad en lugar de la naturaleza (Roca, 2020). En este escenario, la

inteligencia, característica esencial de la humanidad, ha sido desplazada por la inteligencia artificial desarrollada por las computadoras.

4.2 La ley orgánica de datos personales

Durante el gobierno de Lenín Moreno se implementó el Plan Nacional de la Sociedad de la Información y el Conocimiento 2018-2021, el cual incluyó como uno de sus objetivos principales la promulgación de la Ley Orgánica de Protección de Datos Personales. En septiembre de 2019, se presentó a la Asamblea Nacional el proyecto de esta ley con el fin de regular y salvaguardar el derecho a la protección de los datos personales. Tras ser discutido en febrero de 2021, la ley fue finalmente publicada en el Registro Oficial No. 459 el 26 de mayo de 2021, constando de 12 capítulos, 77 artículos, 9 disposiciones generales, 4 transitorias y disposiciones derogatorias.

La Ley Orgánica de Protección de Datos Personales y Derechos Digitales tiene como objetivo regular el ejercicio de los derechos de protección de datos y autodeterminación informativa, así como otros derechos digitales. Esta ley se aplica a los datos personales en cualquier formato, excluyendo los datos domésticos, anónimos y de personas públicas.

En cuanto a su alcance territorial, la ley se aplica cuando el tratamiento de datos se realiza en Ecuador, el responsable o encargado del tratamiento tiene domicilio en el país o si el tratamiento se realiza en personas ubicadas en territorio nacional. Por otro lado, la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos sustituye la definición de accesibilidad y confidencialidad, enfatizando este último como uno de los pilares de la protección de datos personales (Asamblea Nacional del Ecuador, 2021).

Las partes interesadas en los datos personales de acuerdo con la ley son: Las infracciones contempladas en la normativa se dividen en cuatro categorías: a) Infracciones leves cometidas por el responsable, b) Infracciones graves cometidas por el responsable, c) Infracciones leves cometidas por el encargado y d) Infracciones graves cometidas por el encargado.

El Plan Nacional de la Sociedad de la Información y del Conocimiento 2018-2021 considera fundamental la promulgación de una Ley Orgánica de Protección de

Datos Personales para garantizar derechos constitucionales. Asimismo, el Plan Nacional de Gobierno Electrónico resalta la importancia que tiene para el Estado proteger la información y los datos personales en su tercera estrategia (Martínez, et.al, 2023, p.10).

Otra normativa relacionada con la protección de datos personales es la Ley de Telecomunicaciones y su reforma (2015), su propósito es regular a nivel nacional la instalación, operación y desarrollo de la transmisión de diversos tipos de información a través de diferentes medios. Asimismo, se encuentra la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial el 17 de abril de 2002, y la Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada el 18 de mayo de 2004.

Esta última tiene como objetivo garantizar y regular el ejercicio del derecho a la información de las personas, en concordancia con las garantías establecidas en la Constitución y tratados internacionales. Los objetivos de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos están descritos en su Artículo 2.

Es decir, cumplir con lo establecido en la Constitución de la República acerca de la publicidad, transparencia y rendición de cuentas a la que están sujetas todas las entidades estatales y las personas que ocupan cargos públicos, así como garantizar la organización y divulgación de la información sobre la gestión pública.

Además, cumplir con los tratados internacionales firmados por el país en esta materia, permitir la fiscalización de la administración pública y proteger la información personal en manos tanto del sector público como privado. Todo esto con el objetivo de promover la democratización de la sociedad ecuatoriana, el estado de derecho y el acceso a la información pública, así como facilitar la participación ciudadana en la toma de decisiones y su fiscalización.

4.3. El Servicio De Rentas Internas y el Derecho a los datos personales

4.3.1. Política de datos personales en el SRI

La Constitución de la República señala en su artículo 393 que el Estado, mediante políticas y acciones coordinadas, debe garantizar la seguridad de sus

ciudadanos. Esto con el fin de asegurar una convivencia pacífica, fomentar una cultura de paz y prevenir la violencia, la discriminación y la comisión de delitos. La responsabilidad de planificar y ejecutar estas políticas recae en órganos especializados situados en diversos niveles de gobierno.

Las políticas públicas se encuentran enunciadas como garantías constitucionales. En el título III, bajo el nombre de "garantías constitucionales", específicamente en el capítulo segundo titulado "Políticas públicas, servicios públicos y participación ciudadana" (Asamblea Nacional, 2008), se incluyen las políticas públicas. Así, el artículo 85 de la Constitución establece que la formulación, ejecución, evaluación y control de las políticas y servicios públicos deben garantizar los derechos reconocidos por dicha Constitución.

En cuanto a las políticas de privacidad que maneja el Servicio de Rentas Internas tiene la finalidad de garantizar que la información personal recopilada a través de diferentes medios de contacto del Servicio de Rentas Internas se utiliza en sus procedimientos, se maneja con cuidado y se protege de acuerdo con la normativa legal. Esta información solo se comparte de acuerdo con lo establecido en el artículo 99 del Código Tributario (2005). Además, información sobre la identificación de la persona que utiliza el medio digital, incluyendo datos de autenticación, dirección IP y, en caso de ser necesario por motivos de seguridad, detalles sobre el dispositivo utilizado y la ubicación.

El Servicio de Rentas Internas emplea la información personal con el propósito de procesar solicitudes, brindar soporte, ofrecer información relevante, cumplir con procesos de control tributario, administrar servicios, evaluar el uso de productos y servicios, comunicarse sobre eventos o conferencias, otorgar reconocimientos, proteger contenidos y obtener retroalimentación del usuario (Servicio de Rentas Internas, 2024). Además, se pueden recabar datos de autenticación, dispositivo utilizado y ubicación del ciudadano que accede al canal electrónico, si es necesario.

El Servicio de Rentas Internas examinará y actualizará la Política de Privacidad cuando sea necesario, en caso de cambios significativos, se informará a través de un aviso en este sitio web antes de que entren en vigor, de igual manera el SRI, puede utilizar la información personal, incluidos los datos obtenidos durante

la navegación del sitio, para personalizar el contenido, mejorar la calidad del sitio y monitorear la efectividad de los servicios proporcionados. No se compartirá la información personal sin autorización (Servicio de Rentas Internas, 2024).

El Servicio de Rentas Internas protege la información de sus usuarios mediante un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema garantiza la confidencialidad, integridad y disponibilidad de la información, siguiendo las mejores prácticas y estándares internacionales.

Para la protección de datos personales y la prevención de filtraciones, el SRI utiliza un Sistema de Gestión de Protección de Datos Personales (SGPDP). Este sistema se basa en la Norma ISO 27701[3], que proporciona directrices específicas para la gestión de la privacidad, y también toma en consideración otros marcos de referencia importantes, como la Norma ISO 27000[4], que aborda aspectos generales de la seguridad de la información, y el Esquema de Gobernanza de la Seguridad de la Información (EGSI).

Además, el SRI aplica recomendaciones y prácticas de seguridad propuestas por el Open Web Application Security Project (OWASP) para mitigar amenazas y vulnerabilidades en aplicaciones web. Todo esto se complementa con el uso del protocolo HTTPS en sus canales electrónicos, asegurando una comunicación segura y cifrada entre los usuarios y los sistemas del SRI.

El enfoque integral del SRI en materia de seguridad y privacidad permite minimizar riesgos y garantizar un entorno seguro para la gestión de información y datos personales de sus usuarios. Este texto busca ofrecer una explicación más clara y completa sobre las medidas de seguridad implementadas por el SRI, dando contexto a cada sistema y estándar utilizados. También enfatiza la importancia de cada práctica en la protección de la información y la seguridad de los usuarios.

[3] ESGinnova Group (2020) “la ISO/IEC 27701 ayuda a las organizaciones a estructurar y gestionar eficazmente la privacidad de la información, asegurar la confianza de los interesados (clientes, empleados, socios) y cumplir con los requisitos legales y reglamentarios en materia de protección de datos”.

[4] ESGinnova Group (2020) “la serie ISO/IEC 27000 ofrece un conjunto integral de normas y directrices para establecer un ambiente seguro y confiable para la gestión de información crucial para el éxito y la sostenibilidad de cualquier organización”.

El Servicio de Rentas Internas fundamenta la manera en que trata y protege los datos personales de los ciudadanos en la Ley Orgánica de Protección de Datos Personales, publicada en el quinto Suplemento del Registro Oficial No. 459 de 26 de mayo de 2021. Por lo cual, será solamente responsable del manejo de los datos personales que obtenga directamente a través de los canales de atención disponibles para el público, no asume ninguna responsabilidad por el uso indebido de la información por parte del usuario a través de este canal electrónico, por lo tanto, no se hace responsable de la veracidad o precisión de la información enlazada a otros sitios web o proporcionada por terceros.

4.4. Políticas de protección de Datos

4.4.1. Una visión comparada de la protección de datos

En la Constitución de Chile, la protección de los datos personales se apoya en el artículo 19, que garantiza el respeto a la vida privada y la honra de las personas. Por su parte, en la Constitución de Colombia, el artículo 15 establece el derecho a la intimidad y al buen nombre, así como el acceso, actualización y rectificación de la información recopilada en bases de datos públicas y privadas, siempre respetando las libertades y garantías constitucionales (Mok, 2010).

El derecho a la protección de datos de carácter personal no está explícitamente contemplado en la Constitución de Costa Rica, pero el artículo 24 garantiza la protección de la intimidad del hogar, las comunicaciones y los documentos privados, dejando que la ley regule aspectos como las interceptaciones telefónicas y el secuestro de documentos (Sanmartín, 2022). Este artículo establece que las comunicaciones y documentos privados de los habitantes de la República son inviolables.

En México, el artículo 16 de la Constitución establece que nadie puede ser perturbado en su integridad personal, familiar, en su domicilio, documentos o posesiones. También regula situaciones como los registros, inspecciones en el hogar, la exhibición de documentos personales y la violación de la correspondencia (Mok, 2010). Aunque no hace mención directa a la protección de datos personales, se refiere al derecho a la privacidad.

> El artículo 2°, inciso 6) de la Constitución Política de Perú de 1993 garantiza que los servicios informáticos, computarizados o no, tanto públicos como privados, deben proteger la intimidad personal y familiar, evitando suministrar información que la afecte. Además, el artículo 200°, inciso 3) de la misma constitución establece la protección del derecho al "Hábeas Data" como un recurso contra cualquier acción u omisión de autoridades, funcionarios o personas que vulneren los derechos contemplados en los incisos 5, 6 y 7 del artículo 2° (Sanmartín, 2022).

De acuerdo a la normativa vigente en Perú, el derecho a la información ante una entidad pública tiene como límite el respeto a la intimidad personal. Además, la Constitución protege el secreto bancario y la reserva tributaria, los cuales solo pueden levantarse mediante solicitud del juez, el Fiscal de la Nación o una comisión investigadora del congreso, de acuerdo a la ley y solo si se relacionan con el caso en investigación. También se reconocen los derechos a la intimidad, el honor y la propia imagen, y se garantiza la reserva e inviolabilidad de las comunicaciones y documentos privados, los cuales solo pueden ser accedidos por orden fundamentada del juez, con las garantías establecidas por la Ley.

CAPITULO 5: POLÍTICA DE DATOS PERSONALES EN EL SRI

De acuerdo con las políticas respecto de los datos personales que maneja el Servicio de Rentas Internas, tienen entero cuidado respecto de la finalidad y el uso de los datos personales de los contribuyentes, así como sus derechos, tratamiento y protección. Esta política se extiende a todos los datos personales recibidos a través de los procesos institucionales y los canales de atención disponibles para la ciudadanía.

Los datos personales obtenidos a través de los distintos canales de atención ofrecidos por el Servicio de Rentas Internas son utilizados para el cumplimiento de sus funciones de acuerdo a lo establecido por la Ley, sin embargo, solo pueden ser compartidos siguiendo lo dispuesto en la normativa tributaria vigente (Servicio de Rentas Internas , 2023). Asimismo, se recopilan datos de identificación de los usuarios que acceden a los canales electrónicos por motivos de seguridad, como datos de autenticación, dirección IP y, en caso necesario, información del dispositivo y ubicación.

El Servicio de Rentas Internas utiliza la información personal con el fin de procesar solicitudes, brindar soporte, ofrecer información personalizada, realizar controles tributarios, administrar servicios, evaluar el uso de productos y servicios, comunicarse sobre eventos, otorgar reconocimientos, proteger contenidos, obtener retroalimentación y recopilar datos de identificación de los usuarios del canal electrónico, como datos de autenticación, dispositivo utilizado y ubicación, si es necesario.

De igual forma, el SRI reconoce que los titulares de la información tienen derechos sobre el tratamiento de sus datos personales, como el acceso, rectificación, cancelación y oposición. El derecho de acceso permite a los titulares obtener información detallada sobre sus datos personales de manera gratuita. Además, tienen el derecho de solicitar la rectificación de datos inexactos o incompletos, la eliminación de sus datos personales y oponerse al tratamiento de los mismos.

En vista de la evolución de la tecnológica, el SRI manifiesta que, estará en constante revisión y actualización respecto de su Política de datos personales en caso de ser necesario. Por ende, también priorizan a los contribuyentes, manteniendo la idea de que, en caso de realizar modificaciones significativas, se informará a través de un aviso en este sitio web antes de que dichos cambios entren en vigencia, por medio de la página https://www.sri.gob.ec/web/intersri/home fin de obtener respuestas e información sobre las nuevas prácticas de privacidad.

Desde una perspectiva jurídica, este enfoque cumple con las regulaciones locales e internacionales sobre protección de datos y privacidad, incluyendo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en la medida en que sea aplicable. La adhesión a estas normas y regulaciones no solo protege los derechos de los titulares de los datos personales, sino que también proporciona un marco de cumplimiento que puede ser auditado y certificado por terceros, ofreciendo así mayor transparencia y confianza tanto a los ciudadanos como a los organismos reguladores.

La política de protección de los datos personales de los ciudadanos en el SRI se desarrolla bajo las disposiciones de la Ley Orgánica de Protección de Datos

Personales, puesto que, mediante la aceptación de Términos y Condiciones de uso, el portal proporciona información sobre la gestión del Servicio de Rentas Internas y algunos datos estadísticos pueden estar disponibles en formatos abiertos.

Finalmente, respecto a la responsabilidad del SRI en relación a los datos personales, únicamente queda bajo su responsabilidad el manejo y uso de los datos personales que recoja directamente a través de los medios de contacto disponibles, se deslindan de cualquier responsabilidad por uso inapropiado de este canal electrónico. Tampoco se hacen responsable por la veracidad de la información en enlaces a otros sitios web o proporcionada por terceros, además recalcan en que está totalmente prohibido dañar, modificar o interferir con los canales electrónicos, así como acceder de manera no autoriza

CAPÍTULO 6: PROPUESTA DE POLÍTICA INTERNA PARA EL MANEJO DE DATOS PERSONALES EN EL SERVICIO DE RENTAS INTERNAS (SRI)

6.1. Introducción

De acuerdo con las disposiciones constitucionales actuales la protección de datos personales es una obligación por parte del Estado Ecuatoriano, el Servicio de Rentas Internas si bien es cierto, es una institución autónoma e independiente del Estado, permite que mediante su gestión se cumpla con el más alto deber del Estado, el cual es, garantizar la prestación de servicios públicos para el ejercicio y garantía adecuada de los Derechos del individuo, considerando que la tributación es uno de los pilares fundamentales del gasto público, tal institución albera información personal de los contribuyentes mismas que debe ser protegida.

El Servicio de Rentas Internas (SRI) de Ecuador, en cumplimiento con la Constitución de la República del Ecuador y la Ley Orgánica de Protección de Datos Personales (LOPDP), actualmente cuenta con una política de privacidad publicada en su página web garantiza la protección y el tratamiento adecuado de los datos personales de los contribuyentes y empleados. Además, esta política, tiene por objetivo asegurar la confidencialidad, integridad y disponibilidad de los datos personales, promoviendo la confianza y transparencia en el manejo de la

información. Sin embargo, se encuentran algunas falencias que ponen en peligro los datos personales y el tratamiento mismo de aquellos.

En primer lugar, en cuando a la confidencialidad y seguridad de los datos de los contribuyentes, aunque se menciona que los datos personales serán tratados y almacenados con medidas de seguridad y confidencialidad, no se detallan las técnicas específicas ni los estándares de seguridad aplicados. Esto puede generar dudas sobre la efectividad de las medidas de protección implementadas.

Por otro lado, el acuerdo de responsabilidad y uso de medios electrónicos implica que el sujeto pasivo acepta y autoriza al SRI a administrar, sistematizar, procesar y archivar sus datos personales. Sin embargo, la aceptación de estos términos puede no ser completamente voluntaria o informada, ya que es un requisito para acceder a los servicios del SRI.

Además, no se menciona un mecanismo claro para la actualización y mejora continua de la política de protección de datos. La falta de un proceso de revisión y actualización regular puede resultar en políticas desactualizadas que no aborden adecuadamente las nuevas amenazas y desafíos en la protección de datos personales.

Respecto del ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) como trámite interno de número SRI-015-04-01 del catálogo de trámites requiere cumplir con varios requisitos, lo que puede dificultar el proceso para los ciudadanos. Además, el formulario y los canales habilitados para realizar estos trámites pueden ser ingresados de manera presencial por ventanilla o de manera digital por el portar SRI en línea, siendo este último complicado para aquellos usuarios que no manejan la tecnología.

De igual forma, la Política de Privacidad del SRI no menciona explícitamente los principios rectores, lo que podría generar problemas en cuanto a la transparencia y el cumplimiento de las normas de protección de datos. Por lo que es necesario implementar todos los mecanismos adecuados que puedan garantizar un manejo eficiente y protector de los datos personales del contribuyente.

6.2. Justificación

La implementación de una nueva política interna para el Servicio de Rentas Internas (SRI) en relación con el manejo de datos personales es crucial debido a las deficiencias detectadas en la política actual. La necesidad de esta actualización se fundamenta en varios aspectos clave que justifican su urgencia y pertinencia.

En primer lugar, la protección de los datos personales es un derecho fundamental que debe ser garantizado por cualquier entidad que maneje información sensible de ciudadanos. La política vigente carece de medidas exhaustivas para salvaguardar esta información, lo que potencialmente expone a los individuos a riesgos de privacidad y seguridad. Una política más completa permitirá al SRI no solo cumplir con las normativas nacionales e internacionales sobre protección de datos, sino también generar mayor confianza entre los contribuyentes.

Además, la digitalización progresiva y el aumento en el volumen de datos recabados y procesados por el SRI exigen un marco de seguridad robusto y adaptable a nuevas amenazas. Dados los cambios tecnológicos y los crecientes métodos de ciberataques, es imprescindible que la política interna contemple protocolos actualizados para la gestión, almacenamiento y protección de datos. Esto incluye la adopción de tecnologías avanzadas, la implementación de procesos de auditoría regular y el establecimiento de medidas de respuesta ante incidentes de seguridad.

Asimismo, una política más completa y detallada permitiría una mejor gestión interna del SRI, fomentando la transparencia y la eficiencia operativa. La claridad en las responsabilidades y procedimientos contribuirá a una mayor coherencia en la gestión de datos y evitará redundancias y errores que puedan derivar en pérdidas de información o acceso no autorizado.

Finalmente, al proponer una política interna más completa sobre el manejo de datos personales, el SRI podrá posicionarse como una institución modelo en términos de ética y responsabilidad en el tratamiento de datos. Esto no solo beneficiará a sus usuarios y empleados, sino que también fortalecerá su

reputación como una entidad confiable y moderna, comprometida con la excelencia en el servicio público.

Por todo lo anteriormente mencionado, es indispensable que el SRI revise y actualice su política interna respecto al manejo de datos personales, garantizando así la protección, confiabilidad y eficiencia en la gestión de la información que custodia.

6.3. Propuesta

Artículo 1. Ámbito de Aplicación

Esta política se aplica a todos los empleados, contratistas y terceros que manejen datos personales en el SRI, así como a todos los sistemas y procesos que involucren el tratamiento de dichos datos, tanto dentro del territorio ecuatoriano como en transferencias internacionales.

Artículo 2. Definiciones

- **Datos Personales:** Información que permite identificar a una persona física, directa o indirectamente.
- **Tratamiento de Datos:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, como la recolección, almacenamiento, uso, modificación, transferencia y eliminación.
- **Responsable del Tratamiento:** Persona o entidad que decide sobre el tratamiento de los datos personales.
- **Encargado del Tratamiento:** Persona o entidad que realiza el tratamiento de datos personales por cuenta del responsable.

4. **Principios para el Tratamiento de Datos Personales**

- **Legalidad:** El tratamiento de datos personales se realizará conforme a la ley.
- **Transparencia:** Los contribuyentes serán informados sobre el uso de sus datos personales.

- **Confidencialidad:** Los datos personales serán tratados de manera confidencial y solo accesibles a personal autorizado.
- **Seguridad:** Se implementarán medidas técnicas y organizativas para proteger los datos personales contra accesos no autorizados, pérdida o destrucción.
- **Minimización de Datos:** Solo se recolectarán los datos personales necesarios para los fines específicos del SRI.

Artículo 3. Derechos de los Titulares de Datos Personales

- **Acceso:** Derecho a conocer qué datos personales se están tratando.
- **Rectificación:** Derecho a corregir datos personales inexactos o incompletos.
- **Eliminación:** Derecho a solicitar la eliminación de datos personales cuando ya no sean necesarios.
- **Oposición:** Derecho a oponerse al tratamiento de sus datos personales.
- **Portabilidad:** Derecho a recibir sus datos personales en un formato estructurado y comúnmente utilizado.

Artículo 4. Tratamiento de Datos

- **Recolección:** Los datos personales serán recolectados únicamente para fines específicos, explícitos y legítimos relacionados con las funciones del SRI.
- **Almacenamiento:** Los datos personales serán almacenados en sistemas seguros y solo durante el tiempo necesario para cumplir con los fines para los cuales fueron recolectados.
- **Uso:** Los datos personales serán utilizados exclusivamente para los fines para los cuales fueron recolectados.

Artículo 6. Obligaciones del responsable y Encargado del Tratamiento de Datos Personales

- **Responsable del Tratamiento:** Asegurar el cumplimiento de esta política y de la normativa vigente en materia de protección de datos personales.
- **Encargado del Tratamiento:** Implementar las medidas de seguridad necesarias y seguir las instrucciones del responsable del tratamiento.

Artículo 7. Clasificación de Bases de Datos

Las bases de datos se clasificarán según su nivel de sensibilidad y el tipo de datos personales que contengan, estableciendo medidas de seguridad adecuadas para cada categoría.

Artículo 8. Generalidades sobre la Autorización

El tratamiento de datos personales requerirá el consentimiento explícito del titular, salvo en los casos permitidos por la ley. El consentimiento podrá ser revocado en cualquier momento.

Artículo 9. Conservación de los Datos Personales

Los datos personales serán conservados solo durante el tiempo necesario para cumplir con los fines para los cuales fueron recolectados. Una vez cumplidos dichos fines, los datos serán eliminados, bloqueados o anonimizados.

Artículo 10. Protección de Datos por Terceros

La transferencia de datos personales a terceros se realizará únicamente con el consentimiento del titular o cuando sea requerido por ley, asegurando que el tercero cumpla con las normativas de protección de datos.

Artículo 11. Datos que No Requieren Consentimiento

No se requerirá el consentimiento del titular para el tratamiento de datos personales cuando este sea necesario para el cumplimiento de una obligación legal, la ejecución de un contrato, la protección de intereses vitales del titular, o por razones de interés público.

Artículo 12. Transferencia de Datos Personales de Forma Internacional

La transferencia internacional de datos personales se realizará solo cuando se garantice un nivel adecuado de protección de los datos, conforme a la normativa

vigente. Se requerirá el consentimiento explícito del titular para dichas transferencias, salvo en los casos excepcionales previstos por la ley.

Artículo 13. Reglas Generales

- **Evaluación de Impacto:** Realizar evaluaciones de impacto sobre la protección de datos personales cuando el tratamiento pueda implicar un alto riesgo para los derechos y libertades de los titulares.
- **Notificación de Brechas de Seguridad:** Notificar a la Autoridad de Protección de Datos Personales y a los titulares afectados en caso de una brecha de seguridad que comprometa los datos personales.

Artículo 14. Sanciones y Responsabilidades

- **Infracciones Leves**: Multa de hasta el 0.7% de la facturación anual de la entidad. Ejemplos: No tramitar peticiones de los titulares, mantener políticas de protección de datos inadecuadas.
- **Infracciones Graves**: Multa de hasta el 1% de la facturación anual de la entidad. Ejemplos: Uso de datos para fines no informados, cesión de datos a terceros sin cumplir con la ley, no notificar brechas de seguridad.

Artículo 15. Responsabilidades Civiles

- **Indemnización por Daños y Perjuicios**: Los responsables y encargados del tratamiento deberán indemnizar a los titulares por los daños y perjuicios causados por el mal uso de sus datos personales.

Artículo 16. Responsabilidades Penales

- **Acciones Penales**: Los responsables del tratamiento de datos que incurran en conductas delictivas, como la divulgación no autorizada de datos sensibles, podrán ser sujetos a acciones penales conforme a la legislación vigente.

Artículo 17. Implementación y Monitoreo

- **Delegado de Protección de Datos (DPO)**: Designar un DPO encargado de supervisar el cumplimiento de la política de protección de datos.

- **Capacitación**: Realizar capacitaciones periódicas para el personal sobre la gestión adecuada de los datos personales.
- **Auditorías**: Llevar a cabo auditorías regulares para asegurar el cumplimiento de la política y mejorar continuamente los procesos de protección de datos.

Artículo 18. Consultas y Reclamos

Los titulares de datos personales podrán presentar consultas y reclamos sobre el tratamiento de sus datos a través de los canales establecidos por el SRI. Las consultas y reclamos serán atendidos en los plazos establecidos por la normativa vigente. Esta propuesta de política interna busca asegurar que el SRI maneje los datos personales de manera responsable y conforme a la ley, protegiendo la privacidad de los contribuyentes y manteniendo la confianza en la institución.

Artículo 19. Conservación de los Datos Personales

Los datos personales serán conservados solo durante el tiempo necesario para cumplir con los fines para los cuales fueron recolectados. Una vez cumplidos dichos fines, los datos serán eliminados, bloqueados o anonimizados.

Artículo 19. Protección de Datos por Terceros

La transferencia de datos personales a terceros se realizará únicamente con el consentimiento del titular o cuando sea requerido por ley, asegurando que el tercero cumpla con las normativas de protección de datos.

Artículo 20. Datos que No Requieren Consentimiento

No se requerirá el consentimiento del titular para el tratamiento de datos personales cuando este sea necesario para el cumplimiento de una obligación legal, la ejecución de un contrato, la protección de intereses vitales del titular, o por razones de interés público.

Artículo 21. Transferencia de Datos Personales de Forma Internacional

La transferencia internacional de datos personales se realizará solo cuando se garantice un nivel adecuado de protección de los datos, conforme a la normativa

vigente. Se requerirá el consentimiento explícito del titular para dichas transferencias, salvo en los casos excepcionales previstos por la ley.

Artículo 22. Reglas Generales

- **Evaluación de Impacto:** Realizar evaluaciones de impacto sobre la protección de datos personales cuando el tratamiento pueda implicar un alto riesgo para los derechos y libertades de los titulares.
- **Notificación de Brechas de Seguridad:** Notificar a la Autoridad de Protección de Datos Personales y a los titulares afectados en caso de una brecha de seguridad que comprometa los datos personales.

CAPITULO 7: CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

La protección de datos personales, tal como se establece en la Constitución de la República del Ecuador, no solo es esencial para la garantía de derechos fundamentales como la privacidad, sino que también refleja un compromiso del Estado con el respeto y la promoción de los derechos humanos. Esta protección se manifiesta en una serie de disposiciones que aseguran que la recolección y procesamiento de datos se realicen con el consentimiento explícito de los titulares y que estos puedan acceder y rectificar su información en cualquier momento, asegurando así un control efectivo sobre sus datos. Además, la consagración del derecho a la intimidad y el secreto de la correspondencia refuerza aún más este compromiso.

Por otra parte, la acción de Habeas Data se presenta como una herramienta crucial para defender los derechos de los ciudadanos ante posibles abusos en el manejo de sus datos personales, proporcionando un mecanismo legal para acceder y corregir su información almacenada. Este recurso, junto con la obligación del Estado de garantizar la protección de datos mediante legislación adecuada y medidas de seguridad, crea un entorno jurídico robusto que protege la información personal y la privacidad de los individuos.

El análisis del manejo de la política de privacidad del Servicio de Rentas Internas (SRI) de Ecuador revela que, si bien la institución cuenta con medidas para

proteger los datos personales de los contribuyentes y empleados, existen aspectos que requieren atención y mejora. La falta de detalles sobre las técnicas y estándares de seguridad aplicados genera incertidumbre sobre la eficacia de estas medidas, y la aceptación de términos de uso sin una comprensión completa puede comprometer la voluntariedad de los usuarios. Además, la ausencia de un mecanismo claro para la actualización continua de la política y la complejidad en el ejercicio de los derechos ARCO señalan áreas claves que necesitan fortalecimiento.

7.2. Recomendaciones

Para mejorar la protección de datos personales en Ecuador, se recomienda que el Estado continúe fortaleciendo su marco normativo, asegurando que las leyes estén actualizadas y alineadas con las mejores prácticas internacionales en materia de protección de datos. También sería beneficioso implementar programas de capacitación y concienciación para todos los servidores públicos y actores relevantes sobre la importancia de proteger los datos personales y los mecanismos disponibles para ello.

Es importante también promover la creación de una autoridad independiente de protección de datos que supervise y garantice el cumplimiento de las normativas relacionadas con la recolección, almacenamiento y uso de datos personales. Esta entidad debería contar con los recursos necesarios para llevar a cabo auditorías, recibir quejas y aplicar sanciones en caso de incumplimiento, asegurando así una vigilancia continua y efectiva del cumplimiento de la legislación de protección de datos en Ecuador.

Para mejorar la protección de datos personales en el SRI, se recomienda la implementación de un proceso detallado y transparente que explique las técnicas específicas y los estándares de seguridad aplicados a los datos personales, asegurando confianza y transparencia en el manejo de la información. También es crucial establecer una revisión regular y actualización de la política de privacidad, garantizando que esté alineada con las amenazas y desafíos actuales en la protección de datos. Facilitando también el acceso y uso de los derechos ARCO mediante la simplificación de los trámites y proporcionando

asistencia tecnológica a los usuarios menos familiarizados con estas herramientas.

Bibliografía

Agustín, G. J. (2012). *Constitucionalismo en Ecuador.* Ecuador-Quito : Corte Constitucional del Ecuador para el Período de Transición Quito.

Asamblea General de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. París: OHCHR.

Asamblea Nacional. (2008). Constitución de la República del Ecuador. *Registro Oficial 449*. Obtenido de Obtenida de: https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asamblea Nacional del Ecuador. (14 de junio de 2005). Código Tributario. *Registro Oficial Suplemento 38*. Obtenido de Obtenido de: https://www.ces.gob.ec/lotaip/2018/Agosto/Anexos-literal-a2/CODIGO%20TRIBUTARIO.pdf

Asamblea Nacional del Ecuador. (2015). Ley Orgánica de Telecomunicaciones. *Registro Oficial Nº 439*. Obtenido de Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de datos personales. *Registro Oficial Suplemento 459*. Obtenido de Disponible en: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Banco Central del Ecuador . (enero de 2024). *bce.fin.ec*. Obtenido de bce.fin.ec: https://www.bce.fin.ec/component/k2/politica-para-el-tratamiento-de-datos-personales

Benoit, M. B. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO.

Revista chilena de derecho y tecnología, 397-414. doi:http://dx.doi.org/10.5354/0719-2584.2022.67205

Bettoch, M. P. (2018). EL EJERCICIO DE LOS DERECHOS ARCO EN LA VIOLENCIA DE GÉNERO VIRTUAL, ESPECIAL REFERENCIA AL DERECHO AL OLVIDO. *Revista Vasca de Derecho Procesal y Arbitraje*. Obtenido de https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=02147246&AN=133541937&h=Rephg%2BlaaS9p95bBAFmHQWPpQA3RULNRKt3inidkApSkCWKDPrRu9PLQFrXPDb45Ijwfhe%2FU0p2W1Js0fdx0Xg%3D%3D&crl=c

Blanco, J. N. (2018). Reglamento General de Protección de Datos (RGPD) y BIG DATA. *Actualidad civil*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6437479

Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios constitucionales*, 87-120. doi:http://dx.doi.org/10.4067/S0718-52002020000200087

Córdoba, A. G., Leal, S. A., Camargo, D. B., & Ríos, D. R. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, 271-294. Obtenido de https://scielo.isciii.es/scielo.php?pid=S1886-58872020000300017&script=sci_arttext

González, A. G. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de derecho comparado*. Obtenido de https://www.scielo.org.mx/scielo.php?pid=S0041-86332007000300003&script=sci_arttext#notas

Instituto Nacional de Estadística y Censos. (15 de octubre de 2020). *ecuadorencifras.gob.ec*. Obtenido de ecuadorencifras.gob.ec: https://www.ecuadorencifras.gob.ec/institucional/politica-datos-personales/

Luna, J. P. (2019). Aviso de privacidad integral para ejercer derechos ARCO. *National Institute of Public Health*. Obtenido de https://policycommons.net/artifacts/1546459/aviso-de-privacidad-integral-para-ejercer-derechos-arco/2236214/

Macén, A. G. (2021). El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. *CUADERNOS DE DERECHO TRANSNACIONA*, 209-232. doi:https://doi.org/10.20318/cdt.2021.6256

Martínez, M. R., López, J. A., Cevallos, D. P., & Burgos, G. P. (2023). La protección de datos personales en Ecuador. *Estudios Del Desarrollo Social: Cuba Y América Latina*. Obtenido de https://revistas.uh.cu/revflacso/article/view/3594

Martínez, R. (2017). Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos. *Dilemata*, 151–164. Obtenido de https://dilemata.net/revista/index.php/dilemata/article/view/412000105

Mok, S. C. (2010). Privacidad y protección de datos: un análisis de legislación comparada. *Diálogos Revista Electrónica de Historia*, 111-152. Obtenido de https://www.scielo.sa.cr/scielo.php?pid=S1409-469X2010000100004&script=sci_arttext

Proaño, N. C. (2021). ¿Es Contrario el Concepto de Información Pública Previsto en la Legislación Ecuatoriana al Derecho Constitucional a la Protección de Datos de Carácter Personal? Un Análisis de la Sentencia No. 839-14-Ep/21 de la Corte Constitucional del Ecuador. *USFQ Law Working Papers*. Obtenido de https://ssrn.com/abstract=3846519

Rivera, B. (2023). La importancia de la protección de datos y la situación actual del Ecuador. *Revista Cálamo*, 112–122. doi:https://doi.org/10.61243/calamo.13.166

Roca, A. P. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, 165–194. doi:https://doi.org/10.5944/rdp.108.2020.27998

Salvador, W. (2022). Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicos en vícimas ecuatorianas. *Revista mundo financiero. Volumen 3.*, 45. Obtenido de http://www.mundofinanciero.indecsar.orgDerecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicosenvíctimas ecuatorianasThe right to privacy and cybercrime. Social and economic effects on Ecuadorian victimsWashington Manuel Salvador Quiñ

Sanmartín, K. L. (2022). La Protección de datos en el Euador, un análisis en el Derecho comparado. *Universidad Regional Autónoma de los Andes (UNIANDES)*. Obtenido de https://dspace.uniandes.edu.ec/bitstream/123456789/14552/1/USD-DER-EAC-028-2022.pdf

Secretaria de Educación Superior, Ciencia, Tecnología e Innovación. (octubre de 2023). *educacionsuperior.gob.ec*. Obtenido de educacionsuperior.gob.ec: https://www.educacionsuperior.gob.ec/politica-datos-personales/

Segarra, E. (2011). Derecho a la intimidad. Análisis a la normativa ecuatoriana. *Repositorio Institucional Universidad de Azuay*. Obtenido de http://dspace.uazuay.edu.ec/handle/datos/5520

Servicio de Rentas Internas . (12 de Octubre de 2022). *SRI*. Obtenido de SRI: https://www.sri.gob.ec/politica-de-privacidad

Servicio de Rentas Internas . (14 de septiembre de 2023). *sri.gob.ec*. Obtenido de sri.gob.ec: https://www.sri.gob.ec/politica-de-privacidad#pol%C3%ADtica

Servicio de Rentas Internas. (12 de Octubre de 2024). *Derechos de protección de datos personales*. Obtenido de https://www.sri.gob.ec/politica-de-privacidad

Valdiviezo, A. (2021). Delito de violación a la intimidad por medios telemáticos en el Ecuador. *Repositorio Institucional de la Universidad de Guayaquil*. Obtenido de http://repositorio.ug.edu.ec/handle/redug/57943

Vivar, S. A., Ochoa, N. V., Guamán, C. R., & Molina, A. L. (2020). Habeas data y protección de datos personales en la gestión de las bases de datos.

Revista Universidad y Sociedad, 244-251. Obtenido de http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt