ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

ANÁLISIS DE LA PRIVACIDAD EN ECUADOR

ANÁLISIS DE BRECHAS DE PRIVACIDAD EN ECUADOR PRODUCTO DE REGULACIÓN DE TRANSPARENCIA

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

CRISTIAN JHEISON PAGUAY CHIMARRO

cristian-paguay@hotmail.com

DIRECTOR: ANA FERNANDA RODRIGUEZ HOYOS

ana.rodriguez@epn.edu.ec

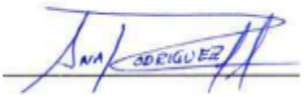
DMQ, septiembre 2022

CERTIFICACIONES

Yo, Cristian Jheison Paguay Chimarro declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

CRISTIAN JHEISON PAGUAY CHIMARRO

Certifico que el presente trabajo de integración curricular fue desarrollado por Cristian Jheison Paguay Chimarro, bajo mi supervisión.



ANA FERNANDA RODRIGUEZ HOYOS

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

CRISTIAN JHEISON PAGUAY CHIMARRO

ANA FERNANDA RODRIGUEZ HOYOS

DEDICATORIA

El presente trabajo va dedicado a Dios, por su guía y bendición durante esta etapa de mi vida, y por permitirme cumplir una de mis metas.

A mis padres, que han sido mi principal apoyo y fortaleza; por el trabajo, sacrificio y amor que me han brindado durante toda mi vida y permitirme ser lo que soy. ¡Son los mejores padres, es un orgullo y bendición ser su hijo!

A mi hermano, a mis abuelitos y a mi mejor amiga, que siempre han estado presentes para apoyarme en cualquier momento que he necesitado.

AGRADECIMIENTO

Agradezco primeramente a Dios por brindarme fortaleza durante cada momento de mi vida.

A mis padres, Galo y Yolanda, que son el pilar fundamental para conseguir mis metas; por su sacrificio, apoyo incondicional y confianza puesta en mí; por los consejos, valores y principios que me han transmitido.

A mi hermano, familia, y amigos, que siempre han estado presentes apoyándome en los momentos que los he necesitado.

A la PhD. Ana Rodríguez Hoyos y al PhD. José Estrada Jiménez, quienes han sido un pilar fundamental en mi desarrollo académico y en la realización del presente trabajo.

A cada docente que formó parte de mi transcurso académico en esta prestigiosa Universidad, por sus enseñanzas y por el conocimiento transmitido.

ÍNDICE DE CONTENIDO

RESUMEN

Iniciativas de transparencia y gobierno electrónico han sido fundamentales para el desarrollo de la administración pública en el Ecuador. Esto ha tenido un impacto positivo en los ciudadanos a través de los beneficios que estas iniciativas ofrecen, lo que ofusca de ver los impactos negativos que estas conllevan relacionadas a la privacidad.

Este trabajo analiza esta problemática a partir de la regulación existente en el Ecuador relacionado a estas iniciativas, se analiza la información revelada por estas iniciativas y se identifica los riesgos latentes e impacto a la privacidad de los ciudadanos. Esto se realiza a través del análisis de la información revelada por los sistemas de consulta pública más relevantes del Ecuador, y del apartado de Transparencia de los sitios web de las entidades públicas obligadas por la LOTAIP.

Los resultados de este trabajo se presentan mediante información resumida y gráficos estadísticos que permitan comprender de manera sencilla la problemática presentada y las afectaciones que representan para los ciudadanos en Ecuador.

Finalmente, se propone estrategias que permitan reducir los riesgos e impacto que implican estas iniciativas para los ciudadanos relacionados a su privacidad.

PALABRAS CLAVE: privacidad, protección de datos, datos personales, información personal, transparencia, gobierno electrónico.

ABSTRACT

Transparency and e-government initiatives have been fundamental to the development of public administration in Ecuador. This has had a positive impact on citizens through the benefits that these initiatives offer, which obfuscates seeing the negative impacts that these entails related to privacy.

This paper analyzes this problem based on the existing regulation in Ecuador related to these initiatives, analyzes the information revealed by these initiatives and identifies the latent risks and impact on the privacy of citizens. This is done through the analysis of the information revealed by the most relevant public consultation systems in Ecuador, and the Transparency section of the websites of the public entities obliged by LOTAIP.

The results of this work are presented through summary information and statistical graphs that allow a simple understanding of the problems presented and the effects they represent for citizens in Ecuador.

Finally, strategies are proposed to reduce the risks and impact that these initiatives imply for citizens related to their privacy.

KEYWORDS: privacy, data protection, personal data, personal information, transparency, e-government.

1. DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

A raíz de la regulación que promueve la transparencia de la “información pública” (LOTAIP) en el Ecuador y de las prácticas poco prolijas para proteger datos personales en el país, este componente del proyecto está orientado a analizar sistemáticamente esta problemática. Este análisis consistirá, en principio, en explorar los distintos sistemas y sitios web mediante los que datos personales se estarían exponiendo públicamente, así como el marco regulatorio que lo permite.

A partir de este análisis, se determinarán los ítems de información personal que se publican abiertamente en Internet. También se estimará el potencial impacto para la privacidad producto de la filtración de esta información, es decir, los riesgos derivados relacionados con la privacidad de los ciudadanos, partiendo, por ej., de determinar la cantidad de ciudadanos afectados. Esto incluirá también un análisis simple de los problemas de seguridad de estos sistemas (p. ej., falta de protección frente a consultas automatizadas) que podrían exacerbar el riesgo de privacidad descrito previamente.

Finamente, se propondrán estrategias tanto técnicas como en el ámbito regulatorio, para reducir el impacto a la privacidad de los ciudadanos.

1.1. Objetivo general

Analizar brechas de privacidad producto de regulación de transparencia en Ecuador.

1.2. Objetivos específicos

i. Examinar la legislación ecuatoriana referente a transparencia, gobierno electrónico y protección de datos personales.

ii. Identificar los ítems de información personal de ciudadanos ecuatorianos que se revelan en línea, así como los servicios y mecanismos que se utilizan para ello.

iii. Analizar los riesgos de privacidad derivados de este comportamiento, así como el impacto que podrían tener.

iv. Proponer estrategias para reducir ese impacto.

1.3. Alcance

Inicialmente, se examinará brevemente la legislación ecuatoriana, particularmente en el ámbito de la transparencia y la protección de datos personales, para identificar los

elementos que incentiven la publicación de datos personales y aquellos que promuevan su protección.

Posteriormente, se explorarán, mediante consulta manual, varios de los sistemas de las instituciones públicas más importantes, que ofrecen información personal públicamente y sin restricciones. Así, se identificarán los ítems y tipos de información personal que se revelan en línea, así como las instituciones y los sistemas que se utilizan para ello. Estos datos serán procesados con el fin de clasificarlos de acuerdo con ciertas categorías definidas por la regulación local referente a protección de datos personales. En el proceso, también se determinará si estos sistemas utilizan mecanismos de protección de privacidad o de seguridad.

A partir de la información recolectada, se evaluarán los riesgos de privacidad de los sujetos de los datos publicados, así como el impacto de esos riesgos en términos de la cantidad de sujetos afectados. Finalmente, se propondrán estrategias de protección de privacidad para mitigar ese impacto.

1.4. Marco teórico

A continuación, se presentan algunas definiciones y una breve explicación del marco legal relacionadas con el gobierno electrónico, la privacidad y la transparencia. Además, se presentan algunos mecanismos de ataque y protección a la privacidad.

1.4.1. Definiciones

El concepto más importante relacionado con este trabajo es el de *privacidad*, que puede ser bastante amplio, como ya lo ha manifestado el Tribunal Europeo de Derechos Humanos (TEDH) [1] [2]. Una de esas definiciones plantea a la *privacidad* como la capacidad de decisión que tiene una o varias personas sobre el manejo de la información que se refiriera a ellas [3]. A partir de esta definición se podrá comprender cómo la divulgación de cierta información personal puede afectar su privacidad.

El *derecho a la privacidad* se encuentra incluido en el artículo 12 de la Declaración Universal de los Derechos Humanos (DUDH). En ella se plantea a la privacidad como un derecho innato del ser humano, y que garantiza el desarrollo de su personalidad y de su dignidad en libertad [4]. Es deber de cada Estado garantizar este derecho a través de las diferentes legislaciones nacionales [4].

La *transparencia* es otro concepto fundamental en el desarrollo de este trabajo. En el ámbito ecuatoriano, la transparencia está relacionada con el derecho de las personas al acceso a la información pública [5]. Este concepto se fundamenta en ciertos valores como

honestidad, eficacia y responsabilidad [6], y es muy popular cuando se plantean soluciones anticorrupción. La disponibilidad de información de las instituciones facilita la contraloría social de sus actividades.

El gobierno electrónico o *e-government* se refiere a las iniciativas que incluyen al gobierno, ciudadanos y empresas, para mejorar las comunicaciones, relaciones y servicios que oferta el Estado con la utilización de medios tecnológicos. Estas iniciativas se encuentran orientadas a la optimización continua de la prestación de servicios públicos, permitiendo así un acceso a la información más sencillo [7].

Un *dato personal* es todo dato relacionado con un individuo, tal como identificadores (p.ej., cédula de identidad) o elementos propios de este (p.ej., altura, peso), que podrían ayudar a determinar la identidad de un individuo directa o indirectamente [8].

En este contexto, una categoría muy importante de los datos personales son los *datos sensibles*. Un *dato sensible* es aquel que, tratado indebidamente, puede originar discriminación o violación de los derechos fundamentales [8] de alguien, y que por ello necesita un nivel de protección mayor.

Otro concepto fundamental para el presente trabajo es el de *titular del dato personal*, que es el individuo cuyos datos son objeto de tratamiento [8]. Por otro lado, el *tratamiento de datos personales* es *cualquier* procedimiento efectuado sobre los datos personales [8]. Estos procedimientos incluyen, por ejemplo, recolectar, registrar, almacenar, eliminar, distribuir, ceder, o, en general, cualquier otra forma de uso de estos datos [8].

Finalmente, el concepto de *información pública* se refiere a todo documento creado, obtenido o contenido por una institución pública o persona jurídica en relación directa con el Estado, sin importar el formato en el que este se encuentre [5].

1.4.2. Base legal

La privacidad es un concepto defendido desde los más altos organismos mundiales de derecho internacional (Naciones Unidades, Unión Europea, UNESCO, etc.). De hecho, se reconoce a la privacidad como un derecho fundamental en el artículo 12 de la Declaración Universal de Derechos Humanos [9]. En el ámbito regional latinoamericano, varios países (Argentina, Uruguay, México, Perú, Colombia, etc.) tienen también legislación que busca garantizar este derecho.

De la misma manera, Ecuador tiene una Constitución que, en el artículo 66 [10], garantiza derechos relacionados con la privacidad, así como el derecho a la protección de datos personales, a la intimidad, a la inviolabilidad, y al secreto de la correspondencia. También,

en el artículo 92, la Constitución de la República del Ecuador (CRE) garantiza varios derechos de los ciudadanos sobre la gestión de sus datos, en el marco del derecho de hábeas data. En esa línea, existen también varias leyes que se refieren al derecho a la privacidad y a la protección de datos personales, incluyendo: la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (LCEFMD); el Código Orgánico Administrativo (COA); Código Orgánico Integral Penal (COIP); la Ley Orgánica de Telecomunicaciones (LOT); la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP); y, finalmente, la Ley Orgánica de Protección de Datos Personales (LOPDP).

La *LOPDP* ecuatoriana garantiza los siguientes derechos relacionados con el derecho a la privacidad [8]: derecho de información, derecho de acceso, derecho de rectificación y actualización, derecho de eliminación, derecho de oposición, derecho a la portabilidad, derecho a la suspensión del tratamiento, derecho de consulta, etc. El derecho a la información obliga a los responsables del tratamiento de datos personales a informar al titular varios detalles sobre ese tratamiento (art. 12). La LOPDP también restringe la transferencia o comunicación de datos personales (p.ej., su difusión) a terceros (art. 33), y obliga al responsable a aplicar medidas para garantizar la seguridad de dichos datos y de su tratamiento (art. 37 y 38). También se ofrece al titular el derecho a la eliminación de sus datos o a que se oponga a su tratamiento, por ejemplo, si afectan derechos fundamentales.

En cuanto a la *transparencia,* es un concepto planteado desde altos organismos mundiales de derecho internacional, p. ej., la Organización de Estados Americanos, la Unión Europea, la UNESCO, la CIDH, etc. En este contexto, incluso se llega a reconocer el derecho de los ciudadanos al acceso a la información pública [11], aunque no es parte de la Declaración Universal de Derechos Humanos [9]. En el ámbito regional latinoamericano, varios países (Brasil, Argentina, Chile, Uruguay, México, Perú, Colombia, etc.) tienen también legislación que busca garantizar la transparencia en las administraciones públicas.

De la misma manera, y en esa línea, la Constitución de la República del Ecuador en el artículo 18, garantiza derechos relacionados con el acceso a las fuentes de información libremente [8]. También existen varios artículos de leyes que se refieren al derecho de acceso a fuentes de información, como, por ejemplo: en el COA, el COIP, la LOT, la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (LOSNRDP), la LOPDP y la LOTAIP.

Esta última, la LOTAIP, garantiza directamente el derecho de acceso a la información pública (art. 1). Este derecho se basa en los principios de acceso a la información: publicidad, transparencia, y rendición de cuentas y gratuidad (art. 2, 4). La ley señala la

información que debe difundirse de manera obligatoria desde todas las entidades públicas y privadas que mantengan relación con el Estado (art. 7) [5].

Finalmente, el gobierno electrónico es una estrategia que se fomenta internacionalmente. Varias organizaciones internacionales como la ONU, la CLAC, la OEA, la CEPAL, etc., han establecido lineamientos y principios para la implementación del gobierno electrónico a nivel mundial [12] [13] [14] [15]. En ese contexto, varios países de Latinoamérica han implementado gobierno electrónico junto con su legislación y han ido mejorando su índice de desarrollo de gobierno electrónico (EGDI) [16].

Por su lado, Ecuador ha adoptado el gobierno electrónico a partir de la legislación que garantiza su correcta implementación y administración. Así, la CRE (art. 227) garantiza que el Estado proporcionará servicios eficientes, eficaces y de calidad [10]. Además, existe legislación con directrices y lineamientos para la administración pública en relación con el gobierno electrónico, como, por ejemplo: el COA [17], la LOPDP [8], la LOTAIP [5], la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos (LOOETA) [18] y la Ley Orgánica del Sistema de Registro de Datos Públicos (LOSRDP) [19].

1.4.3. Microdatos

Al estudiar la privacidad, es común referirse a los datos personales como microdatos [20]. Los *microdatos* son aquellos atributos que sirven para describir un individuo. Algunos ejemplos de microdatos son: cédula de identidad, nombres completos, número de historia clínica, número único estudiantil, etc.

Los microdatos pueden ser de varios tipos, que se describen en la Tabla 1.1.

TABLA 1.1. – Tipos de microdatos [21].

Tipo de atributo	Descripción	Ejemplos
Identificadores (I)	Atributos que permiten la identificación inequívoca de un individuo.	- Cédula de identidad - Nombres completos
Cuasi-Identificadores (QI)	Atributos que no permiten la identificación directa de un individuo, pero sí con la combinación de varios QI.	- Fecha de nacimiento - Estado civil - Sexo - Origen étnico
Confidenciales (C)	Atributos que contienen información sensible de un individuo, en esta categoría se encuentran los datos sensibles.	- Salario - Estado de salud - Pasado judicial
No confidenciales (NC)	Atributos que no pertenecen a ninguna de las categorías anteriores.	- Número de trámite

1.4.4. Tipos de ataque a la privacidad

Dependiendo del escenario de ataque a la privacidad (p. ej., cantidad, granularidad de datos disponibles), los principales mecanismos de ataque se describen a continuación.

Para empezar, el ataque de *identificación* busca identificar de manera inequívoca a un individuo dentro de una población específica. Esto puede conseguirse a través de la obtención de un identificador único (número de identidad), pero también mediante la agrupación de varios cuasi-identificadores del individuo cuya combinación llega a ser única. Una vez identificado un individuo, es posible asociar a éste todos los datos que estén etiquetados con la identificación correspondiente.

El ataque de *clasificación* tiene por objeto clasificar a un individuo en una categoría o grupo de individuos que compartan una determinada característica en común o dispongan de un parámetro comparable (p. ej., personas de negocios con problemas legales). [22]

La *vigilancia* o *seguimiento* tiene por objeto analizar el comportamiento de un individuo a través de los movimientos (físicos o virtuales) que este realice. En general, esto es posible mediante la utilización de datos de ubicación (o datos que permitan inferirla) o datos de estado obtenidos periódicamente como: lugar, fecha, hora, de diferentes actividades realizadas, compras, interacción con redes sociales, ocurrencia de eventos especiales, etc., es decir todo aquello que permita monitorear el comportamiento de un individuo.

El *perfilamiento* es otra actividad que, aunque muy útil para actividades como la publicidad personalizada, podría atentar contra la privacidad. El perfilamiento consiste en construir un perfil de un individuo a partir sus datos. Este perfil refleja, p. ej., las preferencias, intereses, miedos de un individuo y podría utilizarse para hacerle daño.

1.4.5. Mecanismos de protección

La mejor manera de proteger datos personales es evitando su divulgación, especialmente en línea. Ya que muchas veces es necesario enviarlos a un tercero no confiable, la estrategia debe ser minimizarlos, es decir revelar la menor cantidad que sea posible. Un mecanismo común de protección es reducir la precisión de los datos para que puedan “confundirse” con los de otros individuos. Estos mecanismos se describen a continuación.

La *supresión* de datos consiste en eliminar directamente datos, particularmente los más sensibles, como los identificadores. Aunque esto ayuda, un atacante podría identificar un individuo al combinar cuasi-identificadores.

La *generalización* permite limitar la precisión de los datos que se revelan [23], específicamente de los cuasi-identificadores. Esto se realiza a través del remplazo de ciertos valores por valores más generales, como se muestra en el ejemplo de la Figura 1.1. Otra forma de generalizar es dividir los datos en subcategorías y publicarlas en lugar de los datos. Por ejemplo, el valor de una deuda se lo puede subdividir en niveles: bajo ($0 - $1000), medio ($1001 - $10000) y alto (>$10000); evitando así publicar valores específicos. Otro ejemplo es la técnica de micro-agregación *k*-anónima [24], que toma registros de similares características y los reemplaza por valores de medidas resumen tales como: media, mediana, moda, rango, etc. Así, la edad de una persona que tiene 23 y la de otra que tiene 27 se podrían remplazar por una edad promedio de 25 o por un rango de edad de 20-30.

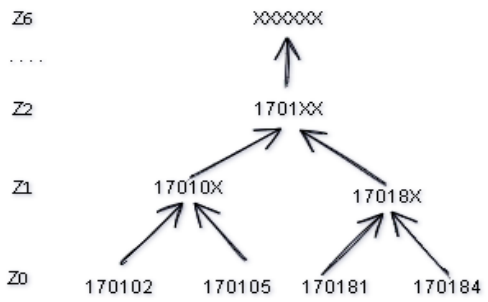


Figura 1.1. Ejemplo de generalización

En el contexto de este trabajo, un mecanismo de protección evidente es el de la *restricción de acceso* a los datos personales solamente, de modo que solo los titulares de esos datos puedan disponer de ellos. Muchas veces estos datos se publican en línea sin justificación adecuada. Adicionalmente, cuando es necesaria su publicación, podría registrarse el acceso a los mismos en una bitácora para verificar si luego son mal utilizados.

1.4.6. Servicios de seguridad

En el contexto de este trabajo, se comprobará que mucha información personal está disponible mediante sistemas de consulta pública. Más allá de la publicación de los datos, hay prácticas muy riesgosas que exacerban el riesgo de privacidad. Los efectos de estas prácticas pueden mitigarse aplicando algunos servicios que están más orientados a la seguridad de los sistemas que a la privacidad de la información. Estos servicios se describen a continuación.

Si un sistema de consulta de datos es públicamente accesible, la *identidad* del usuario del sistema podría registrarse para luego dar seguimiento al uso de los datos consultados. Esto requeriría la *autenticación* del usuario, es decir la verificación de que el usuario es

quien dice ser [25]. Con base en dicha autenticación, el sistema podría también *autorizar* al usuario el nivel de acceso a los datos personales de otro.

Aunque en el ámbito de este estudio los datos personales se publican por defecto, es conveniente que los sistemas que los alojan prevengan el uso inadecuado de estos datos. Así, la *confidencialidad,* mediante el cifrado, debería asegurarse con el fin de proteger especialmente la información sensible. Igualmente, ya que se trata de información oficial (que será tomada como correcta siempre), debería asegurarse que los datos que se publican mantengan su *integridad.*

El abuso de sistemas que entregan información a sus usuarios podría llevar a que estos entreguen información más allá de la permitida. Esto podría conseguirse haciendo consultas automatizadas *(bots)* o pocas consultas genéricas que vuelquen buena parte de una base de datos. Para evitarlo, hay varios mecanismos. Por ejemplo, existen mecanismos de detección de bots basados en el análisis de tráfico, análisis de cookies y, en algunos casos, en la resolución de tareas cognitivas. Uno de esos mecanismos es el de identificación de CAPTCHA [26], que es una prueba para verificar si un usuario que intenta acceder a un sistema es humano o un tipo de robot automatizado que puede ser malicioso [27].

Existen diferentes tipos de CAPTCHA [[27], basados en texto, en audio, en imágenes, en operaciones matemáticas, reCAPTCHA, etc. En la Figura 1.2, se presentan algunos ejemplos.

Figura 1.2. Ejemplos de CAPTCHA

2. METODOLOGÍA

A continuación, se presenta la metodología utilizada para realizar el presente trabajo, así como los diferentes procesos y técnicas usados para obtener los resultados perseguidos. El proceso del presente trabajo se presenta en la Figura 2.1.

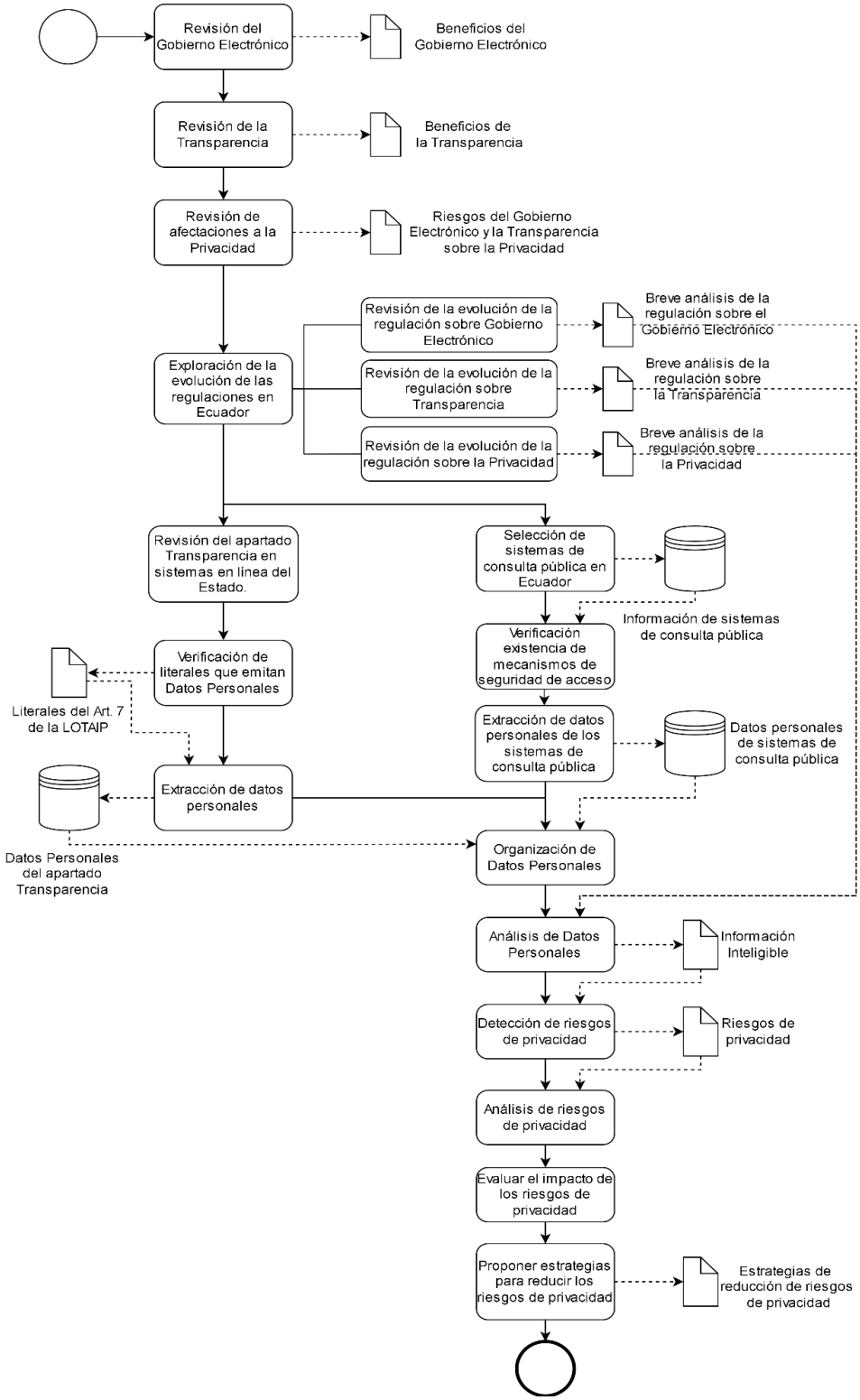


Figura 2.1. Diagrama de Metodología

2.1. Breve análisis de la legislación ecuatoriana en transparencia, gobierno electrónico y protección de datos personales

Como punto de partida para entender la problemática existente con respecto a la privacidad de los ciudadanos en Ecuador, se examinan las iniciativas de transparencia y gobierno electrónico emitidas por el Estado. Para esto, se empieza examinando los principales beneficios que han traído consigo las iniciativas de gobierno electrónico y transparencia que buscan garantizar ciertos derechos y facilitar el acceso a servicios públicos a los ciudadanos. Así también, se examinan algunas actividades que han sido implementadas a la par con la implementación de estas iniciativas, que a su vez pueden convertirse en un riesgo al derecho a la privacidad de los ciudadanos, mismos que se exacerban al ser implementadas por el Estado.

Una vez que se contrastan, a nivel general, los beneficios y riesgos de las iniciativas de gobierno electrónico y transparencia con respecto a la privacidad, se analiza las principales afectaciones o efectos que estas tendrían para la privacidad de los ciudadanos.

A partir de lo anterior, se examina la evolución del gobierno electrónico, la transparencia y la privacidad en el contexto ecuatoriano. En el caso del gobierno electrónico, se analiza la evolución de su implementación con base en el documento "Desarrollo de Gobierno Electrónico en la Administración Pública de Ecuador" emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) en 2018 [28]. En este estudio, se analiza principalmente los cambios ocurridos en las regulaciones existentes o la creación de regulaciones relacionadas al gobierno electrónico. Otro punto que se analiza es la evolución de Ecuador con respecto a los índices internacionales de gobierno electrónico, que a su vez permiten identificar el desarrollo que el país ha tenido en los últimos años y su posición frente a otros países.

Asimismo, se examinan los motivos que llevaron a la implementación de mecanismos de transparencia en el Ecuador y su relación con el gobierno electrónico. Además, se analizan los cambios en regulaciones existentes y las regulaciones creadas a partir de esta iniciativa. En este contexto, se representa y analiza la información que las entidades públicas y privadas que tengan relación con el Estado están obligadas a publicar en sus sitios web por disposición de la LOTAIP [5].

Posteriormente, se revisa la evolución de la garantía de la privacidad y la protección de datos en el Ecuador. Para ello, se examina brevemente la regulación relacionada existente

y la recientemente creada al respecto. En este contexto, se analizan ciertos artículos que se relacionan con la publicación de información personal de los ciudadanos, incluyendo ciertas excepciones. En especial, se analiza la LOPDP y su estrecha relación con la regulación europea de protección de datos [8] [29].

2.2. Obtención de información personal expuesta mediante sistemas de consulta pública

A partir de la problemática presentada en el literal anterior, se procede a obtener la información que se publica en los sistemas de consulta pública implementados a partir del gobierno electrónico; y en el apartado Transparencia de los sistemas web de entidades públicas y privadas en relación con el Estado.

2.2.1. Identificación de sistemas de consulta pública

Para la obtención de información, primero se identifica las entidades públicas ecuatorianas más importantes que podrían albergarlos. La razón es que estas entidades involucran a gran cantidad de ciudadanos, por lo que manejarían un gran volumen de información personal. En este contexto, existen ciertas entidades más pequeñas como los Gobiernos Autónomos Descentralizados (GADs) que también disponen de sistemas de consulta pública similares (*p. ej. el GAD de Rumiñahui*), pero estudiarlos todos llevaría un tiempo superior al previsto.

Para que un sistema de consulta sea considerado un sistema de consulta pública, debe cumplir los siguientes parámetros:

- Ser accesible a través del Internet.
- Pertenecer a una entidad pública.
- Proveer información personal de los ciudadanos mediante consulta en línea.
- No requerir autenticación del titular de la información.

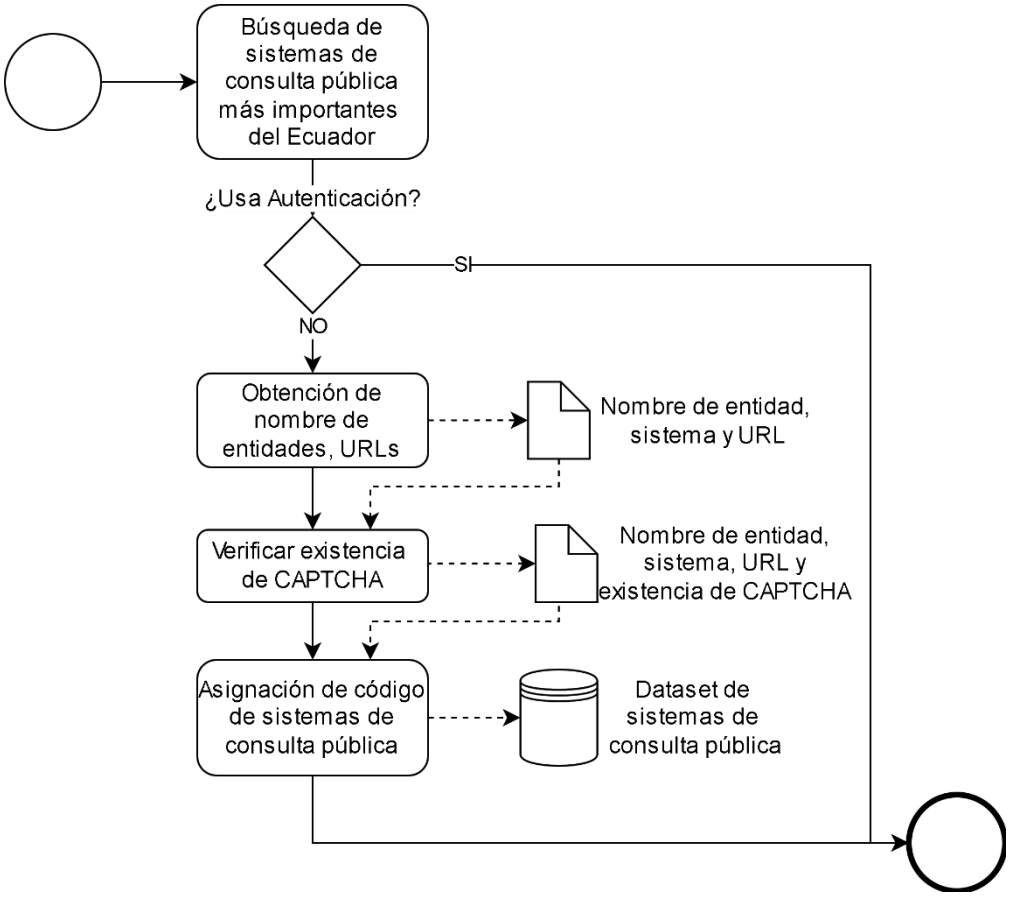


Figura 2.2. Proceso de exploración de sitios para identificación de sistemas de consulta.

Se exploran los sitios web de estas entidades públicas con base en el proceso presentado en la Figura 2.2, buscando los sistemas de consulta que cumplan los requisitos anteriores, y también se los identifica buscando en Google las palabras clave “servicio en línea [entidad] Ecuador”. Luego, se registran la información de los sistemas con los campos: nombre de entidad, nombre del sistema y URL, utilizando un código que incluye las siglas del nombre de la entidad y el número de sistema, debido a que algunas entidades tienen varios sistemas de consulta. También se verifica y registra si existen mecanismos de control de acceso, de control de robots, y si los sistemas son vulnerables a ataques de enumeración.

2.2.2. Identificación de datos personales revelados por los sistemas de consulta

A partir del dataset de sistemas de consulta pública obtenido en el apartado anterior, se obtiene los datos personales más relevantes de cada sistema con base en el proceso presentado en la Figura 2.3.

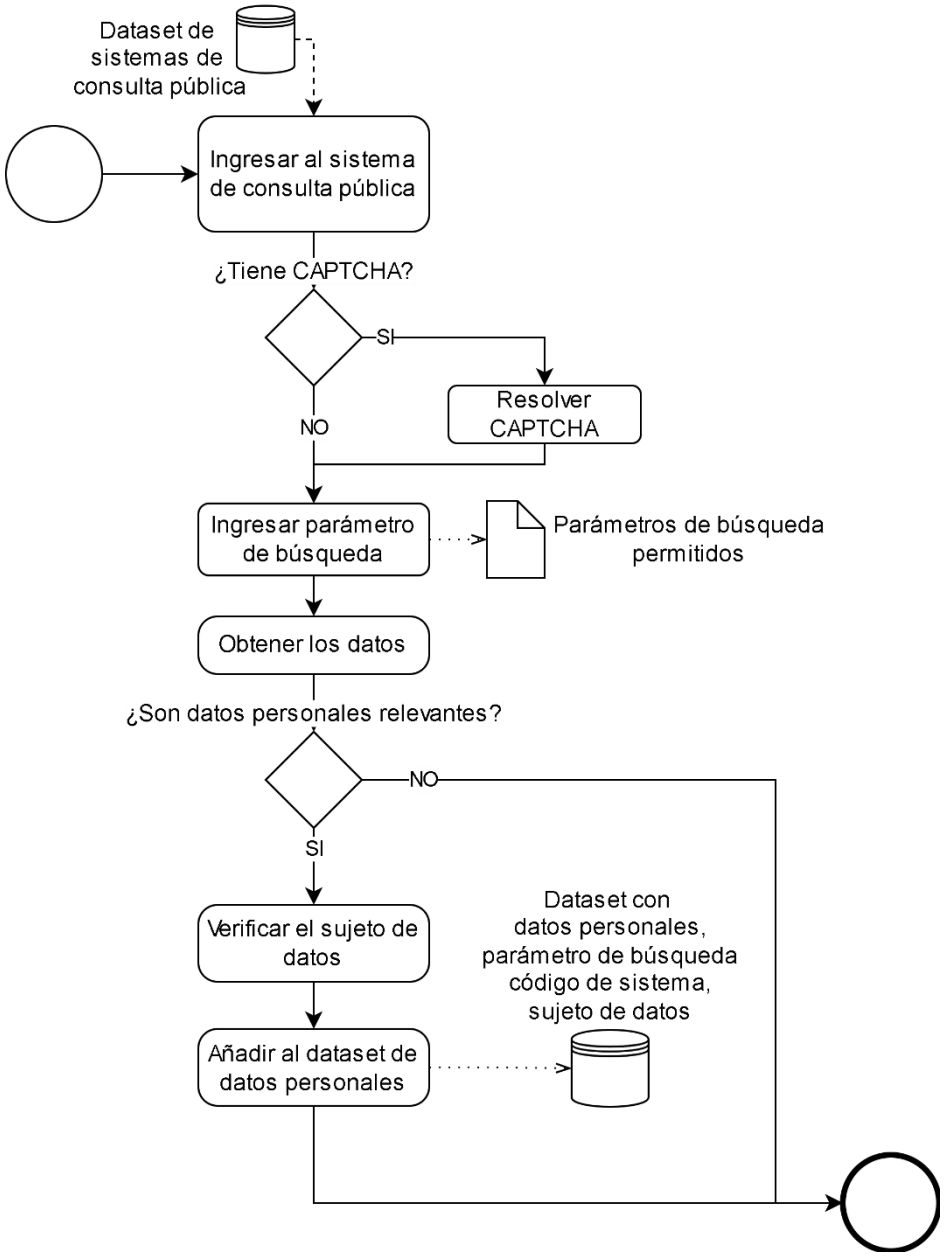


Figura 2.3. Proceso de identificación de datos personales en cada sistema de consulta.

Desde cada sistema de consulta pública, se explora la información que estas revelan, realizando la consulta de información a través de un parámetro de búsqueda (comúnmente identificadores). Estos parámetros de búsqueda se registran junto con un código asignado en un dataset exclusivo para estos. De la información desplegada, se obtiene únicamente los datos personales relevantes y se registran en el dataset de datos personales. Además, de cada dato personal se registra los siguientes campos: dato personal, código de sistema, códigos de parámetros de búsqueda y el sujeto de dato personal. El sujeto de dato personal se refiere a la persona a quien le pertenece los datos personales, en este trabajo se presentan tres posibles escenarios siguientes:

i. **Titular de datos:** se refiere a la persona la cual es objeto de búsqueda.

ii. **Tercero:** se refiere a la persona ajena a la persona objeto de búsqueda.

iii. **Familia:** se refiere a un tercero dentro del círculo familiar del titular de datos.

Cabe destacar que esta identificación corresponde a los *ítems de datos personales* encontrados.

2.2.3. Organización de datos de sistemas de consulta pública

Para facilitar el análisis de la información recolectada, primero, se asigna a cada ítem de dato personal recolectado un nombre de dato personal más general o estándar (p. ej., dirección, ciudad, provincia, se refieren al mismo dato personal, ubicación), esto debido a que varios ítems se refieren a un mismo dato personal. Además, se agrupan los datos personales en categorías (confidencial, demográfico, educación, identificador, judicial, patrimonio, salud y ubicación). Esta organización permite tener una visión amplia de los fenómenos derivados de la revelación de información mediante estos sistemas de consulta pública. Así, se realiza una tabla resumen que organiza los datos en los siguientes campos: categoría de datos personales, datos personales y sujeto de datos personales.

Además, se identifican las categorías especiales de datos personales que se definen en la LOPDP (datos sensibles; datos de niñas, niños y adolescentes; datos de salud; y datos de personas con discapacidad y de sus sustitutos) [8], y se verifica si los datos personales identificados pertenecen a estas categorías. También se verifica si los datos personales corresponden al titular o también a sus familiares o a terceros.

Con este proceso, se obtiene el *dataset de datos personales completo*, el cual contiene los siguientes campos: entidad; código de sistema; ítem de dato personal; dato personal; categoría de dato personal; tipo de dato sensible, tipo de dato de niñas, niños y adolescentes; tipo de dato de personas con discapacidad; sujeto de datos titular; sujeto de datos tercero y sujeto de datos familiar.

2.3. Obtención información personal publicada por disposición de la LOTAIP

2.3.1. Obtención de datos personales

Desde la página web de cualquier entidad pública, se explora la información que estas revelan del apartado transparencia, producto del artículo 7 de la LOTAIP [[5], y con base en el proceso presentado en la Figura 2.4.

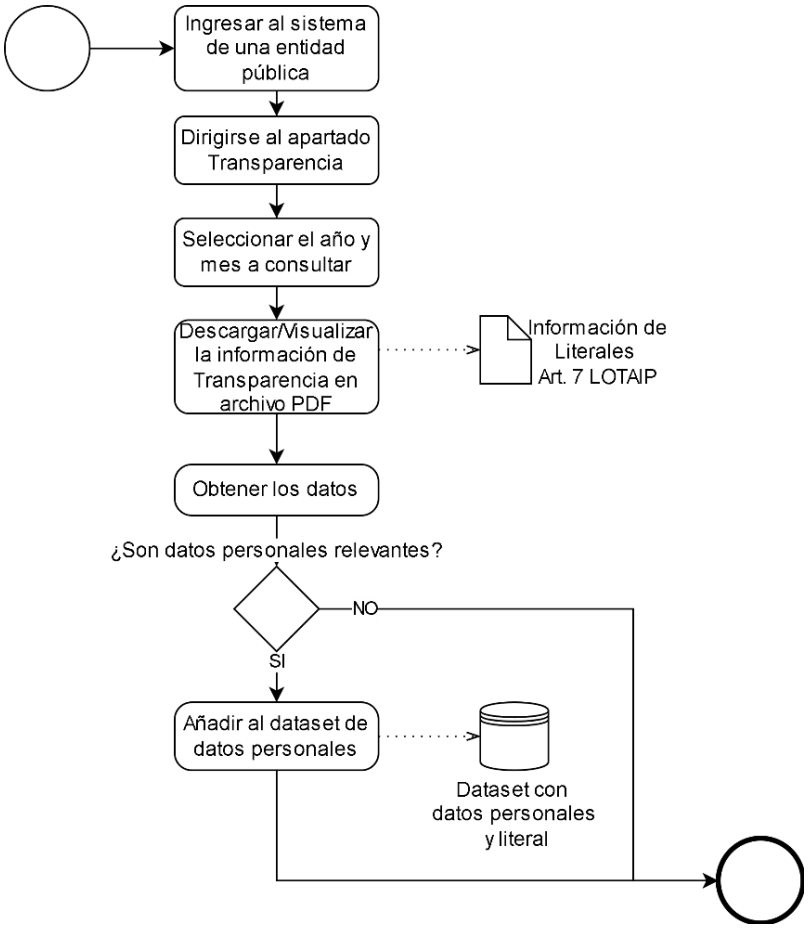


Figura 2.4. Proceso de obtención de información del apartado transparencia

Para esto, se realiza la consulta de información de cada literal, verificando exclusivamente aquellos que emiten información personal de los ciudadanos. De esta información, se obtienen únicamente los ítems de datos personales relevantes y se registra junto con el literal del cual es objeto de consulta. Estos datos se registran en el dataset de datos personales de la LOTAIP.

2.3.2. Organización de datos personales publicados por disposición de la LOTAIP

La organización de estos datos de transparencia se realiza de manera similar al proceso del apartado 2.2.3. En primera instancia, de los ítems de datos personales obtenidos, se les asigna un nombre de dato personal más general y estándar para que la información sea más compacta y fácil de analizar (p. ej., remuneración mensual, remuneración anual, se refieren al mismo dato personal, ingresos).

En esa misma línea, se identifica la categoría de cada uno de los datos personales y se clasifican en las categorías propuestas en el apartado 2.2.3. Con esto, se realiza una tabla resumen con los siguientes campos: categoría de datos personales y datos personales. Además, se verifica cada uno de los datos personales si pertenece a la categoría especial datos sensibles mencionada en la LOPDP [8].

Con esto, se obtiene el dataset de datos personales de la LOTAIP con los siguientes campos: ítem de dato personal, dato personal, categoría de dato personal y tipo de dato sensible.

2.4. Análisis de la información personal publicada en Ecuador debido a iniciativas de gobierno electrónico y transparencia

Como punto de partida, se analiza la información contenida en los datasets de datos personales, tanto de sistemas de consulta pública como de la LOTAIP. Esto se realiza mediante segmentación de los datos para generar información inteligible que permita comprender de manera sencilla la problemática que genera la publicación de información personal debido al gobierno electrónico y la transparencia. A su vez, esto permite identificar los posibles riesgos e impactos que representaría el publicar esta información personal para los ciudadanos.

Concretamente, este análisis nos permite estimar la magnitud de la revelación de datos personales en el país al determinar qué tan común es en las entidades analizadas y cuánta información es revelada.

2.4.1. Análisis de la información de sistemas de consulta pública

En primera instancia, se realiza el conteo del total de entidades públicas que revelan información personal de los ciudadanos; y del total de ítems de datos personales y datos

personales revelados en los sistemas de consulta pública. Estos valores se utilizan posteriormente para realizar gráficos estadísticos, los cuales permiten interpretar la información de manera sencilla. También, son indicadores iniciales de la relevancia de esta práctica de publicación de datos personales.

Por otra parte, se analizan las entidades públicas junto al número de ítems de datos personales y datos personales que revelan cada una de ellas. Este análisis permite encontrar las entidades que más datos personales estarían publicando.

De la misma manera, se analiza las entidades públicas junto al número de ítems de datos sensibles y datos sensibles que revela cada una de ellas. Además, se analizan las categorías de datos sensibles junto al número de entidades públicas que revelan los datos sensibles de cada categoría, se pone especial énfasis en las categorías: salud y pasado judicial. El porcentaje de datos sensibles y el porcentaje de las entidades públicas que comparten datos sensibles, se presentan junto a los análisis anteriores mediante gráficos estadísticos. Este análisis igualmente permite determinar las entidades que más datos sensibles publican en sus sistemas de consulta pública.

En esta línea, se analizan los sistemas que revelan datos personales de niñas, niños y adolescentes junto al número de sistemas que los revelan; las entidades que publican datos personales de niñas, niños y adolescentes junto con el número de ítems de datos personales y datos personales que comparte cada una de ellas. El porcentaje de entidades públicas que comparten al menos un dato de niñas, niños y adolescentes, se presentan junto a los análisis anteriores mediante gráficos estadísticos.

Además, se analiza los sistemas que revelan datos personales de personas con discapacidad, junto con el número de ítems que se revelan de cada uno de ellos. Se presenta este análisis mediante un gráfico estadístico.

Para obtener una visión más amplia del tipo de datos personales que se están revelando en el país, se analizan las categorías de datos personales encontradas junto al número de ítems de datos personales y datos personales revelados en cada una de estas. Por otro lado, se analiza el número de sistemas de consulta pública que presentan: verificación de bots mediante CAPTCHA, vulnerabilidad de ataques por enumeración o mecanismos de protección de privacidad.

Finalmente, se realiza un ranking de entidades públicas con base en las categorías de datos personales revelados mediante sus sistemas de consulta pública. Estas categorías se encuentran organizadas por el tipo de microdatos presentados anteriormente en la Tabla

1.1, y a su vez, se añade la categoría Confidenciales/Categoría Especial (C/CE) que alberga a los datos que pertenecen a ambas categorías. Este ranking lista las entidades públicas ordenadas según la magnitud de los datos personales revelados.

A partir de todo este análisis, se crea un preámbulo a la identificación de los principales riesgos que representa la divulgación de información personal de los ciudadanos.

2.4.2. Análisis de la información de publicada debido a iniciativas de transparencia

Para el caso de la información publicada en los sitios web de las entidades públicas producto de iniciativas de transparencia, se realiza el conteo del total de ítems de datos personales y de datos personales que se publican.

Además, se analizan los literales del artículo 7 de la LOTAIP junto al número de ítems de datos personales y datos personales [5] que la ley dispone que se publiquen. También, se analizan los datos sensibles (según la LOPDP) publicados. A su vez, se analizan los datos personales que más se revelan junto al número de literales del artículo 7 de la LOTAIP que dispone su publicación. Por otro lado, se analizan las categorías de datos personales junto al número de ítems de datos personales y datos personales que se revelan de cada una de estas.

2.5. Discusión sobre los riesgos de privacidad e impacto de las iniciativas de gobierno electrónico y transparencia en Ecuador

A partir de los análisis que se realizan en los apartados anteriores, se explora los posibles escenarios de riesgos de privacidad, en los cuales puede usarse la información personal como insumo para el ataque a la privacidad de los ciudadanos. También se discute el impacto que estarían causando las iniciativas de transparencia y gobierno electrónico en el Ecuador, en términos de vulneración de la privacidad de los ciudadanos.

2.5.1. Riesgos de privacidad

Como punto de partida, se identifican los principales riesgos de privacidad que pueden afectar directa o indirectamente a la privacidad de los ciudadanos. Para esto, se analiza el panorama desde el punto de vista de un atacante, esto con la finalidad de identificar los posibles ataques que pueden efectuarse a la privacidad de los ciudadanos a partir de los sistemas de consulta pública y del apartado de transparencia. Además, se analizan los posibles riesgos de privacidad que implica la falta de mecanismos de control de bots,

mecanismos de control de acceso o mecanismos de protección de privacidad en los sistemas de consulta pública. También se identifican los riesgos de privacidad que implica la libre publicación de información personal en el apartado de transparencia de los sitios web de las entidades públicas.

2.5.2. Impacto en la privacidad de los ciudadanos

Más allá del riesgo de privacidad debido a la publicación de información, producto de iniciativas de gobierno electrónico y transparencia, se analiza también la magnitud del impacto de este problema en el contexto ecuatoriano. Para este ejercicio de reflexión, se intenta por ejemplo determinar la cantidad de individuos que estarían siendo afectados por estas iniciativas, debido a que son aplicadas masivamente desde el Estado y a que las garantías de los derechos de privacidad están sujetas a varias excepciones que los hacen inaplicables cuando los reclaman ciertos grupos de población o cuando los datos personales están en manos de grupos específicos.

2.6. Propuesta de estrategias para reducir el impacto de estas iniciativas en Ecuador

Con base en la información encontrada producto de este trabajo, se proponen líneas de acción orientadas a reducir el impacto previamente analizado. Estas estarán orientadas, en primera instancia, a cuestionar la necesidad de implementar estos sistemas. También se proponen estrategias que se puedan implementar rápidamente, probablemente sin mucho esfuerzo. También se plantea la adopción de mecanismos de protección de privacidad más técnicos que requieren el procesamiento de los datos personales. Por otro lado, se analizan brevemente los mecanismos de protección identificados en los sistemas de consulta pública, destacando sus debilidades.

3. RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1. Resultados

3.1.1. Implicaciones del gobierno electrónico y la transparencia en la privacidad de los ciudadanos

El gobierno electrónico ofrece múltiples ventajas que *benefician* a los ciudadanos. Una de estas ventajas es la optimización del acceso a los servicios y trámites públicos, por ejemplo, permitiendo un acceso más rápido y sencillo a esos trámites. Esto, además, permite una reducción de tiempo y costos. Además, la digitalización de los procesos facilita su auditoría (auditoría social) y permite muchas veces que pueda hacerse por parte de los ciudadanos.

Así también, la implementación de mecanismos de transparencia en el país ofrece varias *ventajas*. Como base del gobierno electrónico, facilita la auditoría social de las entidades pública y, así, la detección de posibles irregularidades [30]. Esto conlleva el aumento del nivel de responsabilidad y participación de las entidades públicas y de los ciudadanos en aspectos relacionados con el Estado [22].

Para obtener los beneficios descritos anteriormente, los mecanismos de gobierno electrónico y transparencia requieren de una gran cantidad de datos personales. Por ello, para conseguirlos, es necesaria la acumulación, procesamiento y hasta publicación indiscriminada de información. De hecho, servicios de gobierno electrónico de mejor calidad usualmente requieren de información más granular y en mayor volumen.

Además, estas iniciativas son implementadas generalmente por el Estado, lo cual amplifica el impacto de la recolección de datos personales. Por ejemplo, el Estado tiene información de todos los ciudadanos, que incluye información muy sensible, y que además puede actualizarse a lo largo del tiempo. Con ello, la magnitud del procesamiento de datos personales en este contexto es masiva y podría servir para construir perfiles detallados y actualizados de los titulares de esos datos.

Esta necesidad de los mecanismos de gobierno electrónico y de transparencia de un gran volumen y granularidad de datos personales podría afectar seriamente a la privacidad de los titulares de esos datos. Por ejemplo, podría permitir identificarlos unívocamente mediante datos como el número de cédula o el nombre completo. Como se indicó en el apartado 1.4.4, la identificación podría servirle a un atacante para asociar un conjunto de datos a un mismo individuo. Esta gran cantidad de información podría usarse también para clasificar a los ciudadanos en categorías que luego faciliten ataques de discriminación, chantaje, acoso, etc. En general, los datos personales podrían ser tan abundantes y

variados en este contexto que permitan crear perfiles de los ciudadanos que reflejen sus movimientos, patrones de comportamiento, etc. Sin duda, la afectación a la privacidad se exacerba por las capacidades y obligaciones del Estado. Al estar obligado a recolectar e incluso a publicar datos personales masivamente, se estaría facilitando la vigilancia o el rastreo a gran escala de los ciudadanos.

3.1.2. El gobierno electrónico, la transparencia y la privacidad en el Ecuador

En este apartado se analizan los efectos en la privacidad de los ciudadanos de la regulación ecuatoriana que incentiva el gobierno electrónico y la transparencia.

En lo que respecta al gobierno electrónico, hay varias iniciativas legales y esfuerzos orientados a incentivar la adopción del gobierno electrónico en el país [31]. Para empezar, en el año 2000 se declara como política de Estado el acceso universal a los servicios de telecomunicaciones, que son el canal para el acceso de los ciudadanos a las herramientas de gobierno electrónico. Luego, en 2003, se publica el primer Programa Nacional de Gobierno Electrónico y Sociedad de la Información con dos componentes: definición de políticas e implementación de proyectos de infraestructura.

En 2007, Ecuador firma la Carta Iberoamericana de Gobierno Electrónico, que plantea garantizar para los ciudadanos la transparencia de las administraciones públicas, la optimización de tiempos, la facilidad de acceso a la información y la participación activa. También en 2007, se crea la Subsecretaria de Informática con el fin de mejorar la gestión de gobierno mediante la implementación de proyectos informáticos.

En 2011, se propone el Plan Nacional de Gobierno en Línea, con el objetivo de promover servicios digitales para ciudadanos, gobiernos y empresa; y de fomentar el acceso ciudadano a la información y servicios públicos, por ejemplo, mediante portales. En esa dirección, en 2013, se crea la Subsecretaría de Gobierno Electrónico con el fin de apoyar en la implementación del gobierno electrónico en la administración pública. También, asociados al gobierno electrónico, se definen por primera vez mecanismos para la simplificación de trámites. En 2014, se lanza el primer Plan Nacional de Gobierno Electrónico 2014 – 2017 con más de 100 programas, proyectos y normas. En 2015, se dispone la *implementación obligatoria* del Plan Nacional de Gobierno Electrónico a todas las instituciones públicas de la Administración Pública Central, Institucional y dependiente de la Función Ejecutiva. En 2016, se oficializa la publicación del Plan Nacional de Gobierno Electrónico 2016 – 2017, cuyos objetivos incluían incrementar el acceso a servicios

electrónicos, el nivel de acceso a la información pública, y la eficiencia, eficacia y desempeño de las entidades públicas.

Por otro lado, en 2017, el Código Orgánico Administrativo ya dispone adoptar instrumentos de gobierno electrónico, mientras que, en 2018, se plantea como política de Estado la mejora regulatoria y la simplificación administrativa y de trámites [32]. También en 2018 se emite el Plan Nacional de Gobierno Electrónico 2018-2021 [33]. Finalmente, en 2019 se promulga la Ley para la Optimización y Eficiencia de Trámites Administrativos, que garantiza la implementación de trámites en línea cuando sea posible.

Fruto seguramente de este gran impulso al gobierno electrónico, a través de regulación y planificación en esa línea, Ecuador cuenta con muy buenos indicadores de desarrollo de gobierno electrónico, incluso comparados con el resto de los países del mundo. El país ha despuntado particularmente en los índices OSI (índice de servicios en línea) y EGDI (indicador de gobierno electrónico), como se muestra en la Figura 3.1 y 3.2 [34] [35] [36]. Estos indicadores son el reflejo del amplio despliegue de servicios en línea en el país durante los últimos años [37], que ha requerido el procesamiento de muchos datos personales y que, como se verá más adelante, viene acompañado de la revelación de esos datos en la misma magnitud.

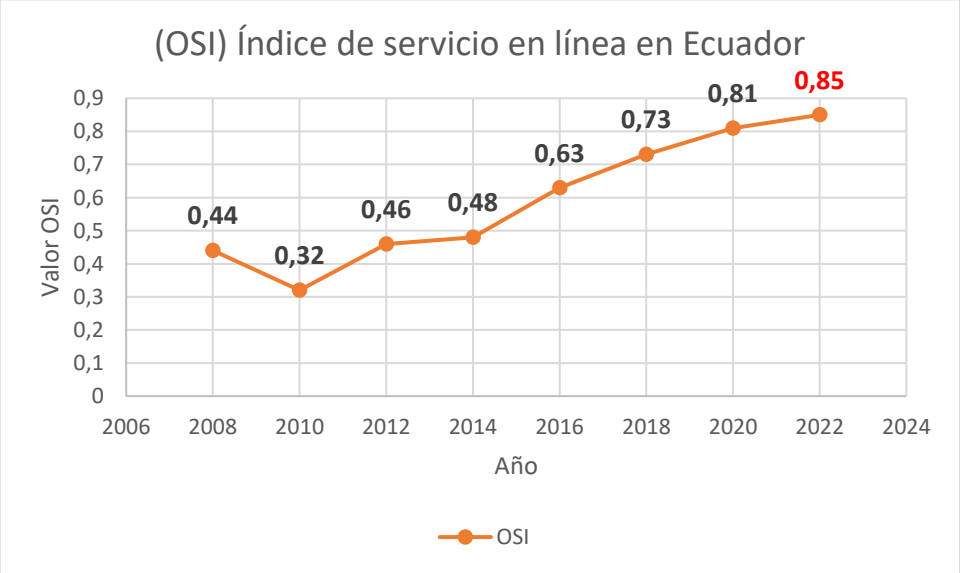


Figura 3.1. Índice de servicios en línea de Ecuador 2006-2022 [33]

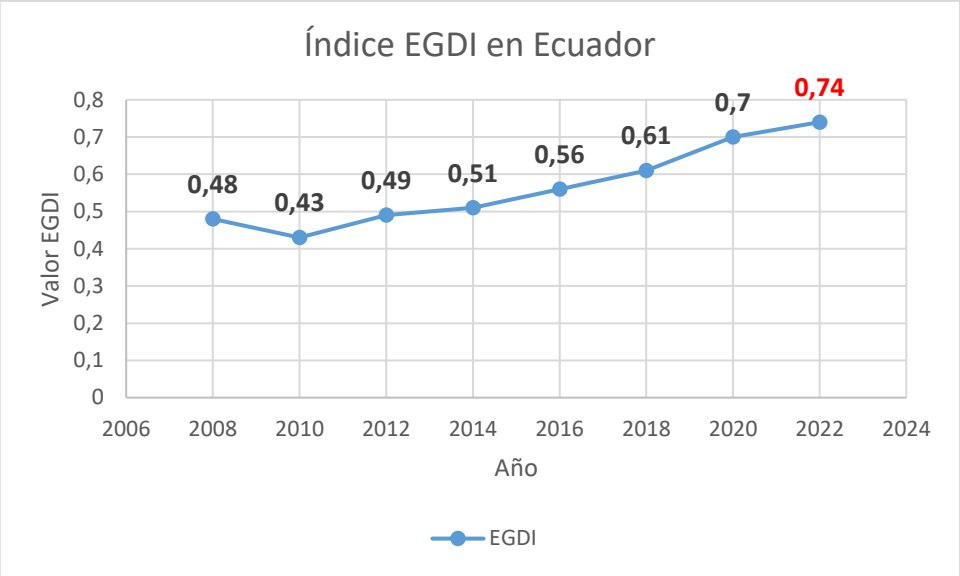


Figura 3.2. Índice de gobierno electrónico de Ecuador 2006-2022 [33]

Junto con el desarrollo del gobierno electrónico en el Ecuador, se han implementado mecanismos de *transparencia* en el sector público, con el afán de combatir la corrupción en el país e incrementar la responsabilidad y participación entre el Estado y la ciudadanía [22]. De hecho, en Ecuador, la transparencia ha sido promocionada como la panacea para combatir la corrupción [38], llegando a subir varios puestos en la calificación global del derecho a la información (puesto 74) [39]. Con el fin de garantizarla, en 2004 se promulgó la LOTAIP y, desde entonces, obliga a las entidades públicas a publicar una gran cantidad de información sobre sus empleados y procesos [5]. Concretamente, 5 literales del artículo 7 de esta ley, que se resumen en la Tabla 3.1, disponen la publicación de información de cada entidad pública, que incluye varios datos personales, particularmente de sus empleados.

La gran cantidad de datos personales que se necesita publicar y procesar para poner estas iniciativas de gobierno electrónico y transparencia a disposición de los ciudadanos tiene graves implicaciones para la privacidad de esos mismos ciudadanos. Esto es así no solo por la granularidad de esos datos, sino también por la cantidad de individuos que se verían afectados. Pero lo más grave es que no existen criterios orientados a proteger esa información.

Tabla 3.1. Literales del art. 7 de la LOTAIP que disponen publicar datos personales [5]

Literal	Información que se dispone a publicar
b1	Directorio completo de la institución
b2	Distributivo de personal
c	La remuneración mensual por puesto y todo ingreso adicional, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes
j	Un listado de las empresas y personas que han incumplido contratos con dicha institución
n	Los viáticos, informes de trabajo y justificativos de movilización nacional o internacional de las autoridades, dignatarios y funcionarios públicos

Como ya se ha explicado, tanta información personal publicada pone en serio riesgo la privacidad de los ciudadanos. Ventajosamente, por un lado, la privacidad y la protección de datos personales ha estado garantizada en Ecuador en varios cuerpos normativos, tal como se describe en la sección 1.4. La Constitución, varias leyes relacionadas con telecomunicaciones, comercio electrónico, de procedimiento penal, tienen referencias a la protección de datos personales. En 2021, se publicó la LOPDP y es actualmente la principal base para el desarrollo de protección a la privacidad de los ciudadanos. Sus principales objetivos son: garantizar el derecho a la protección de los datos personales de los ciudadanos, que los ciudadanos tengan el acceso y decisión sobre su información y sus datos [8]. Cabe destacar que el cumplimiento de estos objetivos se verá reflejado en los próximos años a través de la correcta ejecución por parte de entidades públicas, empresas privadas y ciudadanos.

Aunque la LOPDP está inspirada en el Reglamento General de Protección de Datos europeo (RGDP), tiene varias limitaciones. Una de esas limitaciones se relaciona con las reducidas sanciones con respecto al RGDP. Pero la limitación más importante tendría que ver con las excepciones que la misma ley plantea a su aplicación, fenómeno que ya ocurría con legislación previa. Por ejemplo, la Ley de Comercio Electrónico ya indicaba que el consentimiento para el procesamiento de datos *no es necesario* cuando su recopilación se realiza en *el contexto de la administración pública* [40].

Así también, la LOPDP plantea varias excepciones a los derechos de privacidad de los usuarios en el Ecuador [8]. Por ejemplo, declara como *datos accesibles al público y sujetos de tratamiento* a los datos personales de *servidores públicos* (art. 2) y, aunque enmarca esta declaración al ejercicio de su profesión, competencias, facultades, etc., directamente dispone que sean de acceso público el histórico de su declaración patrimonial y remuneración, que contienen datos personales sensibles. La LOPDP también plantea la excepción de la garantía a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad cuando los datos son insumos del ejercicio del derecho a la libertad de expresión y opinión (art. 18); se entiende que las actividades periodísticas estarían exentas de respetar estos derechos, propios de todos los ciudadanos.

3.1.3. Análisis de información

En este apartado, se realiza el análisis de la información obtenida de los sistemas de consulta pública y del apartado Transparencia de los sitios web de las entidades públicas producto de la LOTAIP.

3.1.3.1. Datos personales obtenidos mediante sistemas de consulta pública

Entre las 21 entidades públicas seleccionadas se encuentran varios ministerios, entidades de control y, en general, instituciones que ofrecen servicios públicos muy concurridos. En los sitios web de estas entidades se identifican 64 sistemas de consulta pública (ver detalle en ANEXO I), que revelan 111 ítems de datos personales, que al estandarizarse corresponden a 78 datos personales. Estos datos personales se encuentran resumidos en la Tabla 3.2.

Cabe destacar que se identifican casos particulares de páginas web y aplicaciones móviles que funcionan como pasarelas a varios de estos sistemas de consulta pública, generando tráfico e ingresos mediante publicidad [41] [42] [43]. Estos son los casos de *EcuadorLegalOnline, EcuadorWeb,* y *Consultas Ecuador*. Estas páginas y aplicaciones web se usan en este trabajo para identificar algunos de los sistemas de consulta pública.

Tabla 3.2. Tabla resumen de datos personales revelados por sistemas de consulta

Categoría	Dato Personal	Sujeto
Identificador	Cédula de identidad	Titular/Tercero/Familia
	Código de nacimiento	Titular/Familia
	Dirección correo electrónico	Titular/Tercero
	Identificador tributario de contribuyente	Titular/Tercero
	Nombres completos	Titular/Tercero/Familia
	Número de usuario	Titular/Familia
	Número placa vehículo	Titular
	Identificador de vehículo	Titular
	Razón social	Titular/Tercero
Demográfico	Edad	Titular/Tercero/Familia
	Estado civil	Titular/Tercero/Familia
	Estatus bono	Titular
	Estatus registro consular	Titular
	Detalles contribuyente	Titular
	Etnia	Titular/Familia
	Detalles de nacimiento	Titular/Tercero/Familia
	Lugar de trabajo	Titular/Tercero
	Monto exoneración por discapacidad	Titular
	Nacionalidad	Titular/Tercero/Familia
	Número de embarazo/hijos	Titular/Familia
	Parentesco	Titular/Familia
	Peso	Titular/Familia
	Sexo	Titular/Familia
	Talla	Titular/Familia
Educación	Curso colegio	Titular/Tercero
	Especialidad	Titular/Tercero
	Estatus becario	Titular
	Detalles de registro de título	Titular
	Lugar estudios bachillerato/pregrado/postgrado	Titular/Tercero
	Nivel de educación/entrenamiento	Titular/Tercero/Familia
	Profesión	Titular/Tercero
	Título	Titular
Laboral	Actividad económica	Titular
	Cargo sector público	Titular/Tercero
	Estatus afiliación al seguro social	Titular
	Estatus impedimento laboral	Titular
	Estatus laboral/empleador	Titular
	Estatus pertenecer a servicios de seguridad	Titular
	Tipo de licencia de conducir	Titular
	Fecha de cambio de estatus laboral	Titular
Salud	Estatus seguro de salud	Titular/Tercero
	Estatus vacunación	Titular
	Número de controles parentales	Titular/Familia
	Número/tipo de parto	Titular/Familia
	Porcentaje de discapacidad	Titular/Tercero
	Tipo de seguro de salud	Titular
	Tipo de discapacidad	Titular/Tercero
	Tipo de sangre	Titular
	Tipo de vacuna	Titular
Ubicación	Fecha/hora de cita	Titular
	Identificador de predio	Titular
	Jornada educativa	Titular/Tercero
	Número de teléfono	Titular/Tercero
	Ubicación geográfica	Titular/Tercero
	Número de turno	Titular
	Lugar de trámite	Titular/Tercero
Patrimonio	Activos por derechos	Titular/Tercero
	Detalles del predio	Titular
	Avalúo vivienda	Titular
	Dinero en efectivo/inversiones	Titular/Tercero
	Avalúo vehículo	Titular
	Estatus accionista/representante legal	Titular
	Estatus deuda	Titular
	Estatus herencias	Titular
	Fondos complementarios	Titular/Tercero
	Información de empresa/acciones/particpaciones	Titular/Tercero
	Cuentas por cobrar	Titular/Tercero
	Deuda	Titular/Tercero
	Valor pago	Titular/Tercero
	Otros detalles vehículo	Titular
	Ingresos/Renta	Titular/Tercero
Judicial	Antecedentes penales	Titular/Tercero
	Detalles denuncias/delitos	Titular/Tercero
	Estatus impedimento de salir del país	Titular
	Procesos judiciales/infracciones	Titular/Tercero
	Prohibición enajenar	Titular
Confidencial	Clave dirección correo electrónico	Titular/Tercero

Al analizar el número de ítems y datos personales revelados por cada entidad, se encuentra que las entidades públicas que más datos personales revelan mediante sistemas de consulta son el Registro Civil (19), el Servicio de Rentas Internas (SRI) (18) y el Consejo de la Judicatura (17), como se muestra en la Figura 3.3. Puntualmente, el Registro Civil y el SRI alojan información de todos los ciudadanos (masiva), mientras que la Contraloría General del Estado, el Consejo de la Judicatura y el Municipio de Quito concentran datos personales de ciudadanos relacionados con un contexto laboral específico (p. ej., empleados públicos, ciudadanos inmersos en procesos judiciales), o geográfico (p. ej., habitantes de una ciudad o provincia).

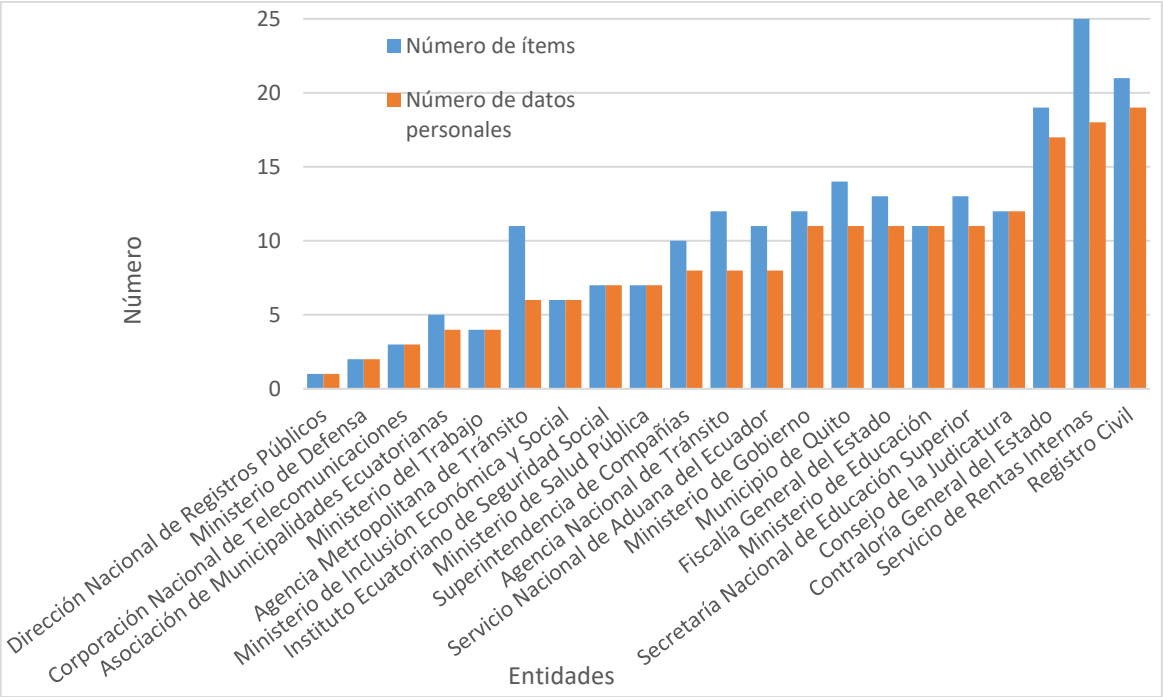


Figura 3.3. Número de ítems y datos personales revelados por entidades públicas.

Con respecto a los datos personales sensibles (según la LOPDP), el 52% de estas entidades revelan al menos un dato sensible en alguna de las categorías etnia, pasado judicial, condición migratoria, y salud; 38% de ellas revelan datos de salud mientras que el 24% revelan datos de pasado judicial (ver Figura 3.5). En este contexto, se revelan datos de procesos judiciales/infracciones, de estatus de seguro de salud, y hasta detalles del proceso de parto de una madre (número de embarazo, número de controles prenatales). Evidentemente, aquellas entidades que más revelan estos datos son aquellas que ofrecen servicios relacionados con estas categorías sensibles, tal como se muestra en la Figura 3.4. De todos los datos personales revelados, el 28% corresponden a datos sensibles.

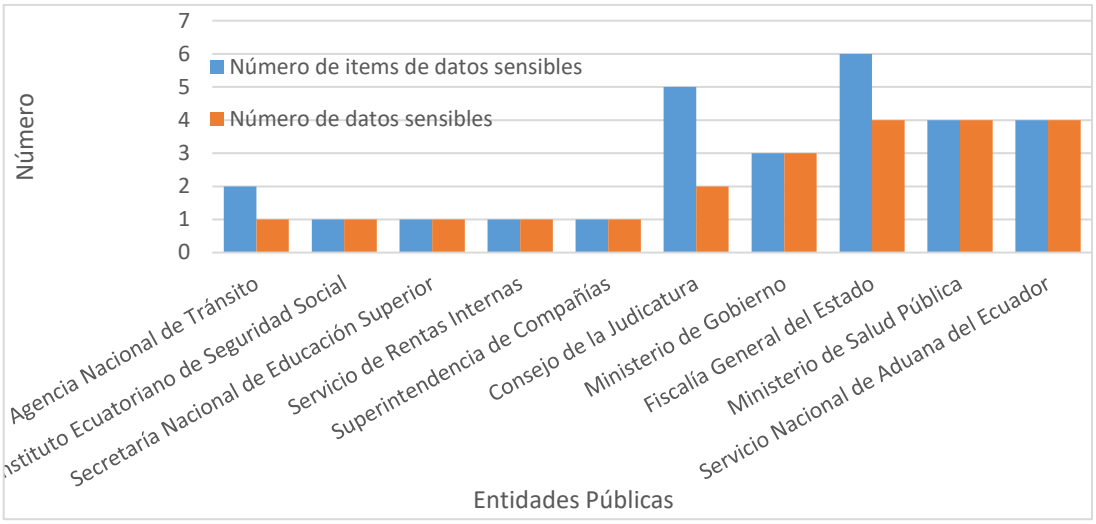


Figura 3.4. Cantidad de ítems y datos *sensibles* revelados por entidades públicas.

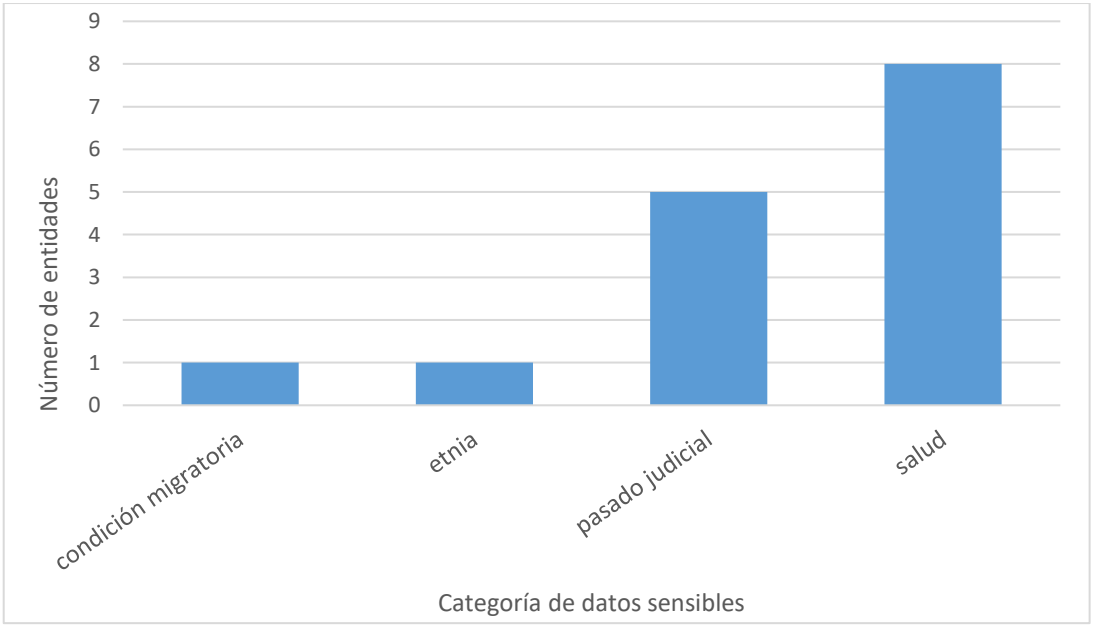


Figura 3.5. Número de entidades por categoría de datos sensibles.

Del análisis de los datos personales de niñas, niños y adolescentes, se encuentra que el Registro Civil (14), el Ministerio de Educación (11) y el Ministerio de Salud Pública (7) son las entidades que revelan más datos de esta categoría (ver Figura 3.6). Además, 57% de las entidades estudiadas revelan al menos un dato personal de niñas, niños y adolescentes, es decir que *más de la mitad de las entidades públicas revelan datos personales de menores de edad*.

En lo que respecta a los datos personales de discapacitados, se encontró un par de sistemas que los revelaban, pero que dejaron de hacerlo durante la realización de este trabajo. Estos sistemas permitían, respectivamente, consultar si un ciudadano recibía el

bono de desarrollo humano y si un ciudadano era sujeto de exenciones de tributos. La información que estos sistemas revelaban incluía estatus bono, nombres completos, tipo de discapacidad, porcentaje de discapacidad, y monto de exoneración por discapacidad.

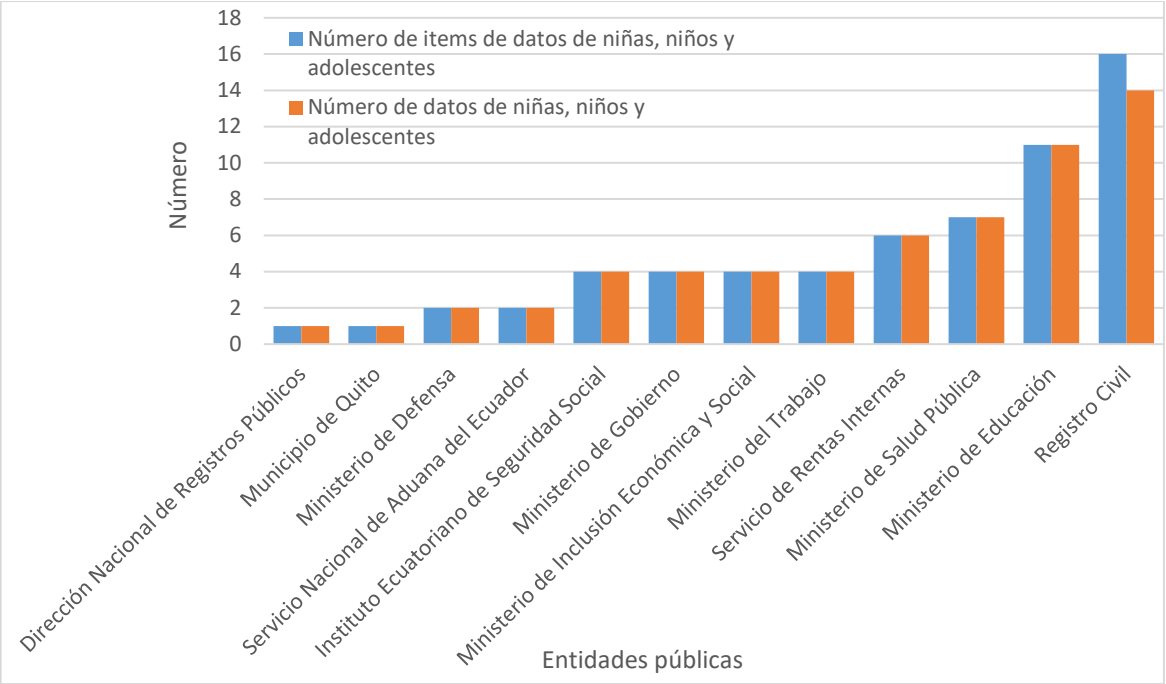


Figura 3.6. Entidades que revelan datos de niñas, niños y adolescentes

Al analizar la magnitud de la revelación de datos por categoría, de acuerdo a la cantidad de datos personales, se encuentra que los que corresponden a patrimonio (16) e identificador (15) son los que más se revelan, tal como se muestra en la Figura 3.7.

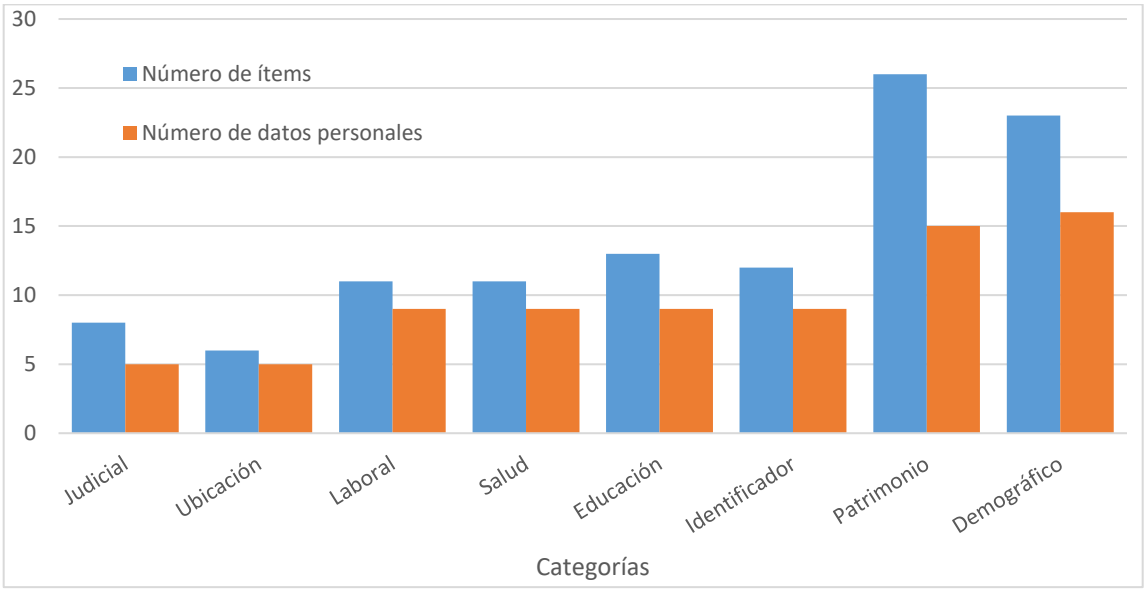


Figura 3.7. Ítems y datos personales revelados por categoría

Por otra parte, como se muestra en la Figura 3.8, estos sistemas de consulta pública no solamente revelan datos personales del titular de los datos, sino *también de familiares y de terceros*.

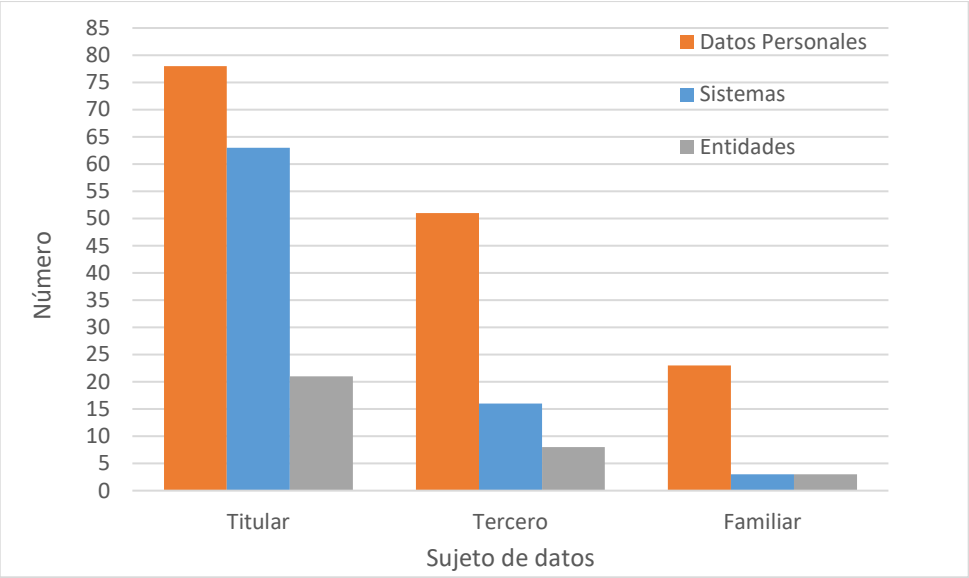


Figura 3.8. Cantidad de datos personales revelados por tipo de sujeto de datos (titular, terceros, familiares).

Finalmente, en lo correspondiente al análisis de los datos personales revelados por sistemas de consulta pública, se elabora una tabla resumen de las entidades públicas, las categorías de datos personales que revelan mediante sus sistemas de consulta, el porcentaje de entidades que revelan esos datos, y el porcentaje de revelación de datos considerando solamente estas categorías como una aproximación del nivel de riesgo de privacidad (Ver Anexo V). A partir de esta tabla se encuentra que las entidades públicas que más categorías de datos personales revelan mediante sus sistemas de consulta son: el Ministerio de Gobierno (62%), la Fiscalía General del Estado (54%), el Ministerio de Educación (54%), el Ministerio de Inclusión Económica y Social (54%), el Registro Civil (54%) y el Servicio de Rentas Internas (54%). Además, se observa que todas las entidades comparten datos de tipo identificador y que más del 50% de las entidades revelan datos sensibles de los ciudadanos. Otras categorías que se comparten en más de la mitad de las entidades son: demográficos (62%) y ubicación (57%).

Más allá de la gran cantidad de datos personales revelados por estos sistemas, el 25% de ellos son vulnerables a ataques de enumeración, es decir que, con una o pocas consultas, se podría obtener resultados de varios individuos. Por ejemplo, consultando por un solo apellido se arrojan resultados de todos quienes comparten ese apellido.

3.1.3.2. Mecanismos de protección de sistemas de consulta pública

Aunque la información de los sistemas de consulta pública es, en muchos casos, sensible y abundante, pocos implementan mecanismos de protección. De estos, solo la mitad tiene un mecanismo de control de bots (CAPTCHA).

Solamente el 6% de sistemas de consulta pública analizados implementa mecanismos muy incipientes de protección de privacidad que, frente a la gran cantidad de datos personales revelados, no aportan significativamente. Una de estas estrategias es la generalización de ciertos datos como el número de cédula o número de motor, reemplazando la parte más específica de esos datos con un símbolo (1717248550→171724XXXX). Otra de las estrategias es agregar una marca de agua con la dirección IP de quien consulta al documento que contiene los datos personales, de modo que se desincentive la difusión de esta información.

3.1.3.3. Datos personales obtenidos mediante iniciativa de transparencia

Del análisis de la LOTAIP, aplicable para todas las entidades públicas del país, se identifican 4 literales del artículo 7 (b, c, j, y n) que disponen la publicación de 25 ítems de datos personales que, al estandarizarse bajo nuestros criterios, corresponden a 17 datos personales (Ver Anexo III).

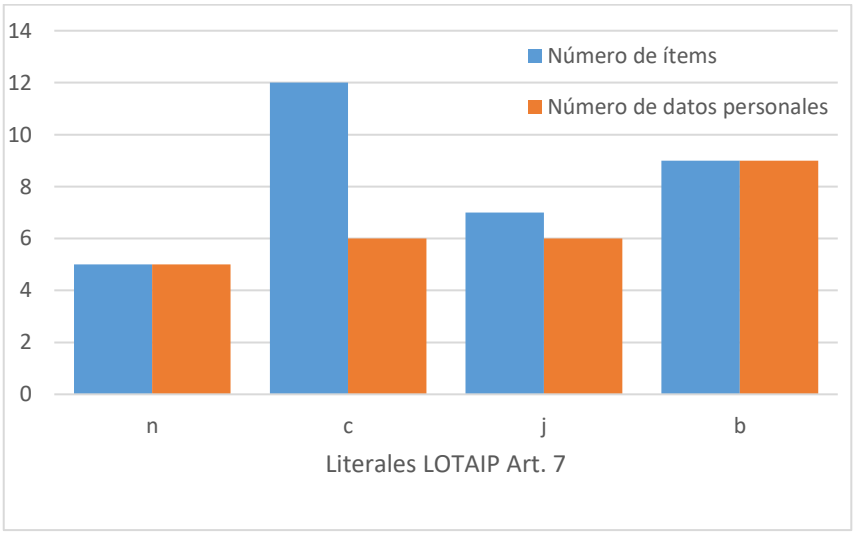


Figura 3.9. Número de datos personales publicados debido a cada literal del art. 7 de la LOTAIP.

La Figura 3.9, muestra la cantidad de datos personales que se obliga a publicar por cada uno de estos literales en el apartado de transparencia de los sitios web de las entidades

públicas. El literal b (Directorio de la institución y Distributivo del personal) es el que estaría permitiendo la revelación de la mayor cantidad de datos personales.

Esta iniciativa legal de transparencia obliga a la publicación de 17 datos personales, entre los que se encuentran nombres completos, cargo en sector público, ingresos, detalles de contrato, y lugar de trabajo. Luego de categorizar estos datos personales, se encuentra que los más revelados corresponden a las categorías de laboral e identificador, aunque también se incluyen datos de ubicación y patrimonio (ver Figura 3.10). Además, se presentan estas categorías junto con sus datos personales revelados en el Anexo IV.

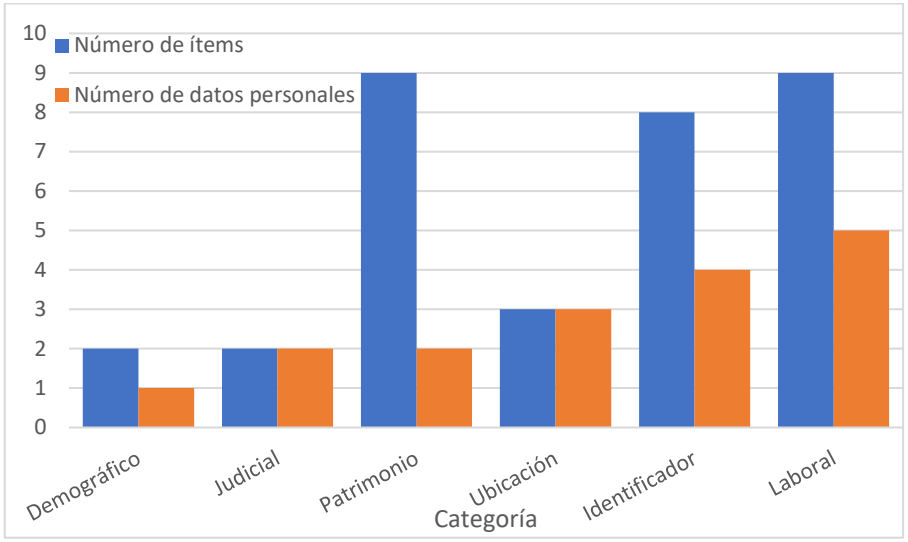


Figura 3.10. Número de datos personales por categoría publicados por disposición de la LOTAIP.

3.1.4. Riesgos e Impacto

Tal como se ha evidenciado en los resultados descritos previamente, en Ecuador se publica deliberadamente muchos datos personales por parte de instituciones públicas en nombre de la transparencia y mediante iniciativas relacionadas con gobierno electrónico. A continuación, se describen los riesgos de privacidad que esto implica.

Primero, en casi todos los casos, se publican datos identificadores que permiten asociar el número de identidad (cédula) con el nombre completo de un individuo y viceversa. En el ámbito de la privacidad, un ataque de identificación, es decir, distinguir inequívocamente a un individuo dentro de una población, usualmente consiste en agrupar los atributos que lo caracterizan de manera general (cuasi-identificadores) y construir con ellos una especie de identificador, dado que los identificadores reales se eliminan por defecto para protección de privacidad. Sin embargo, en el contexto que este trabajo analiza, los identificadores se publican tal cual. En el caso de los sistemas de consulta, de hecho, los identificadores son

el parámetro de búsqueda que permite obtener más información directamente asociada a un individuo. En cuanto a las iniciativas de transparencia, ambos identificadores, número de cédula y nombres completos, se publican juntos. Así, frente a un ataque de privacidad, un atacante que conozca alguno de estos datos podría obtener fácilmente todos los otros que se publican. Si no tuviese alguno de los identificadores, podría encontrarlos en fuentes de terceros como redes sociales, copias de cédula que se entregan para trámites, hojas de vida, u otros documentos públicos como tesis de grado. En consecuencia, a falta de un ataque de identificación, los datos de los ciudadanos se publican directamente asociados a su identidad, lo cual incrementa significativamente el riesgo para su privacidad.

Por otro lado, los datos publicados, y asociados a una identidad, podrían permitir a un atacante *clasificar* o *categorizar* a su víctima. Por ejemplo, los datos de patrimonio (impuestos, ingresos, propiedades) podrían ubicar a un individuo en una categoría que le impida recibir un crédito o, en su defecto, en una categoría que atraiga a criminales interesados en extorsionar, secuestrar o robar objetivos que destaquen por su nivel de ingresos. Así también, los datos de salud o judiciales podrían ser insumo de instituciones que discriminen individuos por el número de hijos que tengan o por procesos judiciales inconclusos.

La gran cantidad de datos personales publicados se puede consolidar para construir un perfil que ofrezca una visión clara de las características de un individuo, a través de diversas facetas de su vida. Así como un investigador criminal construye un perfil de un delincuente para estudiarlo y finalmente atraparlo, el perfilamiento podría servirle a un atacante para vulnerar la intimidad de una víctima.

El riesgo para la privacidad en el escenario de análisis de este trabajo también se incrementa debido a varios factores. (1) Quien se encarga de publicar la información es el Estado, que seguramente posee la mayor cantidad de información de *todos* los ciudadanos. (2) Los datos personales se publican directamente en Internet, incrementando significativamente la cantidad de atacantes potenciales. (3) Algunos sistemas de consulta no controlan la cantidad de registros que se obtienen de las consultas; en ocasiones se vuelca muchos registros a partir de un parámetro de búsqueda genérico (p. ej., si se busca por un apellido, se obtiene información de *todas* las personas con ese apellido). (4) En varios casos, no existen mecanismos mínimos de protección que controlen la extracción automatizada de datos, por lo que hay un riesgo importante de que un atacante pueda obtener esa información fácilmente.

Estos factores que incrementan el riesgo de privacidad para los ciudadanos exacerbarían también las consecuencias de los ataques descritos previamente. De hecho, se estaría constituyendo una virtual plataforma de vigilancia masiva en línea, debido a la magnitud y granularidad de los datos publicados, a la cantidad de individuos involucrados, a la facilidad de acceso a estos datos, pero especialmente a la calidad de estos datos, que incluyen ubicación, patrimonio, salud, etc., y que en muchos casos se actualizan constantemente.

Como resultado, *todos* los ciudadanos (18 millones de ecuatorianos [44]) están a merced de estos ataques de privacidad, incluso grupos que no interactúan periódicamente con los servicios públicos, como los niños (6 millones de niñas, niños y adolescentes [44]); o grupos extremadamente vulnerables como las personas con discapacidad (más de 470 mil personas con discapacidad existentes en Ecuador [45]). En particular está en riesgo el grupo de todos los aproximadamente *400 000 empleados públicos* [46], en el que se encuentran más de 50 000 policías [47], más de 40 000 empleados de las fuerzas militares [49], operadores de justicia, autoridades de rango medio, etc., cuyo poder de decisión en ciertos ámbitos sensibles podría ponerles en mayor riesgo si sus datos están disponibles abiertamente. Este grupo, de acuerdo a las excepciones que plantea la regulación, tendría restringidos sus derechos de privacidad. En contraste, las actividades relacionadas con la libertad de expresión (generalmente periodísticas), que podrían ser desempeñadas por cualquier ciudadano, no estarían obligadas a considerar estos derechos de privacidad, lo que podría generar distorsiones graves en la protección de datos personales.

Considerando que la transparencia y el gobierno en línea se plantean como soluciones definitivas para graves problemas de la sociedad (corrupción, atención del Estado) y dado el impulso y la aceptación ciudadana que ha tenido su implementación en el país, seguramente su adopción seguirá creciendo en los próximos años, con el consiguiente agravamiento de los efectos en la privacidad de los ciudadanos. Así, se irán integrando más instituciones públicas que manejan ingentes cantidades de datos personales, incluyendo los GADs o gobiernos municipales del país.

Finalmente, ciertos detalles surgieren que estos datos personales ya están siendo aprovechados por terceros. Por ejemplo, hay varios sitios en Internet y aplicaciones móviles que concentran el acceso a estos sistemas de consulta pública y, al hacerlo, generan ingresos mediante publicidad en línea. Además, aunque estos sistemas han sido utilizados por periodistas para destapar casos de corrupción en compras públicas o en la emisión de documentos fraudulentos, hay casos en los que estos mismos se utilizan para extraer datos de un objetivo mediático para atacarlo. Por lo tanto, es probable que delincuentes estén

aprovechándose ya de estos datos para llevar a cabo ataques de acoso, chantaje, o extorsión contra determinados individuos.

3.1.5. Estrategias para reducir el impacto

En principio, los mecanismos de protección que ofrecen estos sistemas de consulta, frente a la revelación de datos personales, son bastante incipientes. La mitad de sistemas implementa control mediante CAPTCHA, para evitar consultas automatizadas, mientras solo 4 adoptan mecanismos específicos, muy básicos, y por lo tanto inútiles, de protección de privacidad.

Frente a los riesgos manifiestos a la privacidad que se describen en la sección anterior, se debería, para empezar, analizar la necesidad real de implementar, o de poner en línea, todos esos sistemas.

Se podría también considerar la adopción de mecanismos de control de acceso, que permitan el acceso a los datos solamente a su titular o a un grupo más restringido de usuarios que requieran legítimamente el uso de esos datos. Parte de esta estrategia podría ser registrar el acceso a los datos y particularmente de quien accede (registrando la dirección IP origen, datos de identificación, etc.), de manera que se pueda determinar patrones de uso que ayuden a detectar, por ejemplo, un empleo malicioso de estos datos.

Otra estrategia para evitar el impacto en la privacidad de los ciudadanos consiste en la *minimización de datos*, es decir que se publique lo estrictamente necesario. Para ello, sería necesario reducir en lo posible la cantidad de datos personales que se publican pues los resultados de este trabajo hacen sospechar que hay demasiados datos personales que se publican con excesiva granularidad. Esta estrategia implicaría también un análisis profundo de la necesidad de publicar los datos de todos, o de la mayoría de los ciudadanos. Probablemente, no es necesario publicar datos de niños. En esta línea, se podría también publicar ciertos datos con una reducida especificidad, generalizándolos; los datos identificadores serían los primeros candidatos de implementación de esta estrategia.

Finalmente, sería importante analizar las excepciones del marco legal a la garantía de los derechos de privacidad, así como también sería importante observar que la aplicación de ese marco legal, en cuanto a transparencia y gobierno electrónico, se haga considerando la privacidad de los sujetos de los datos que los sistemas relacionados procesan y publican.

3.2. Conclusiones

Lo expuesto a lo largo del presente trabajo permite concluir lo siguiente:

- Aunque los indicadores de transparencia y desarrollo de gobierno electrónico crecen significativamente, se lo ha conseguido probablemente a costa de la privacidad de los ciudadanos.
- Seguramente se están publicando datos personales que no es necesario publicar, basados en la enorme cantidad de datos revelados que se ha registrado en este trabajo.
- La implementación del gobierno electrónico, a través del despliegue de sistemas de consulta pública, por parte de las instituciones del Estado no considera la protección de la privacidad de los ciudadanos cuyos datos se publican.
- Los riesgos de privacidad descritos se agravan debido a que involucran a poblaciones sumamente vulnerables como la de niños, niñas, adolescentes y la de personas con discapacidad.
- Los mecanismos de protección de privacidad en los sistemas analizados y en la implementación de las iniciativas de transparencia en Ecuador son básicamente inexistentes.
- Existe una amenaza latente hacia los ciudadanos debido a la revelación de información sensible como sus datos judiciales, datos de salud o datos de su patrimonio, lo cual puede traer graves consecuencias como discriminación, chantaje, extorsión o amenazas.
- Dado que estas iniciativas se implementan desde el Estado, los riesgos de privacidad se exacerban hasta el punto de que el despliegue de estos sistemas y la publicación de datos personales estarían dando forma a una virtual plataforma de vigilancia masiva a alcance de cualquier usuario de Internet.
- Las excepciones de la legislación frente a la protección de los datos de empleados públicos y la publicación sin control de sus datos podrían estar poniendo en serio riesgo a una importante parte de la población y particularmente a quienes tienen a su cargo responsabilidades sensibles como policías, personal de salud, operadores de justicia, etc.

- Es importante que el Estado implemente estrategias como las expuestas en este trabajo para garantizar el derecho a la privacidad de todos los ciudadanos, sin restricciones ni excepciones.

3.3. Recomendaciones

- Cualquier solución o servicio que requiera el procesamiento de datos personales debería diseñarse considerando la privacidad de los sujetos de esos datos.
- Es necesario analizar la aplicación de la LOTAIP y su concordancia con la garantía de derechos fundamentales como el derecho a la privacidad.
- Es necesario también analizar si es estrictamente necesario publicar tantos datos personales para ofrecer los distintos servicios en línea.
- Como trabajo futuro, sería interesante evaluar el impacto de la falta de control de interacciones automatizadas sobre los sistemas de consulta pública analizados.
- Una futura línea de trabajo podría dirigirse también a incluir en este análisis de riesgos de privacidad a los sistemas de consulta desplegados por los gobiernos autónomos descentralizados del país.

4. REFERENCIAS BIBLIOGRÁFICAS

[1] TEDH, «Sentencia del Tribunal Europeo de Derechos Humanos,» de *Peck contra Reino Unido, epígrafe 57*, United Kingdom, 2003.

[2] Tribunal Europeo de Derechos Humanos, «DerechosHumanos.net,» 23 08 2022. [En línea]. Available: https://www.derechoshumanos.net/tribunales/TribunalEuropeoDerechosHumanos-TEDH.htm. [Último acceso: 22 04 2022].

[3] A. Westin, «Privacy and Freedom,» 03 01 1968. [En línea]. Available: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr. [Último acceso: 12 02 2022].

[4] «Definición .DE,» 15 01 2022. [En línea]. Available: https://definicion.de/privacidad/. [Último acceso: 12 02 2022].

[5] Asamblea Nacional del Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, Quito: LEXIS, 2004.

[6] CPCCS, «Consejo de Participación Ciudadana y Control Social,» 2022. [En línea]. Available: https://www.cpccs.gob.ec/transparencia-y-lucha-contra-la-corrupcion/transparencia/#:~:text=La%20transparencia%20se%20traduce%20en,las%20instituciones%20p%C3%BAblicas%20y%20privadas.. [Último acceso: 13 02 2022].

[7] L. M. B. Malagon, «E-Government in Digital Era: Concept, Practice, and Development,» *Nacional Institute of Development Administration,* 2002.

[8] P. d. l. R. d. E. Asamblea Nacional, «Ley Orgánica de Protección de Datos Personales,» 2021.

[9] Organización de Naciones Unidas, Declaración Universal de los Derechos Humanos, 1948.

[10] G. d. Ecuador, «Constitución de la República del Ecuador,» Montecristi, 2008.

[11] Fundación Regional de Asesoría en Derechos Humanos, «INREDH, El Derecho a la Información Pública,» 05 2015. [En línea]. Available: https://www.inredh.org/archivos/pdf/derecho_a_la_informacion_publica.pdf. [Último acceso: 14 01 2022].

[12] Organización de Estados Americanos, «Foro Gobierno Electrónico OEA,» 04 2011. [En línea]. Available: http://portal.oas.org/LinkClick.aspx?fileticket=4zRxKXP80Uc%3D&tabid=1729. [Último acceso: 07 2022].

[13] O. d. N. Unidas, «Departamento de Asuntos Económicos y Sociales,» [En línea]. Available: https://publicadministration.un.org/es/ict4d. [Último acceso: 11 07 2022].

[14] A. Naser y G. Concha, «Comisión Económica para América Latina y el Caribe,» [En línea]. Available: https://www.cepal.org/sites/default/files/publication/files/7330/S1100145_es.pdf.

[15] C. L. d. A. p. e. Desarrollo, «Carta Iberoamericana de Gobierno Electrónico,» 2007. [En línea]. Available: https://clad.org/wp-content/uploads/2020/07/Carta-Iberoamericana-de-Gobierno-Electronico.pdf. [Último acceso: 11 07 2022].

[16] O. d. N. Unidas, «E-Government Development Index (EGDI),» [En línea]. Available: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index. [Último acceso: 11 07 2022].

[17] Asamblea Nacional del Ecuador, «Código Orgánico Administrativo,» 07 07 2017. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/11/COA.pdf. [Último acceso: 01 06 2022].

[18] Asamblea Nacional del Ecuador, Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, Quito, 2018.

[19] Asamblea Nacional del Ecuador, «Ley Orgánica del Sistema de Registro de Datos Públicos,» 07 2011. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf. [Último acceso: 23 05 2022].

[20] P. Samarati, «Protección de las identidades de los encuestados en la publicación de microdatos,» 11 2001. [En línea]. Available: https://ieeexplore.ieee.org/document/971193.

[21] AGESIC, «Presidencia de Uruguay - Tecnologías de la Información,» 2020. [En línea]. Available: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Gu%C3%ADa%20sobre%20Anonimizaci%C3%B3n%20de%20Datos%20vf.pdf. [Último acceso: 08 04 2022].

[22] A. R. L. U. J. P. J. F. José Estrada, «Digital Hyper-Transparency: Leading e-Government Against Privacy,» *Escuela Politécnica Nacional,* 2020.

[23] «datos.gob.es,» Gobierno de España, 25 10 2021. [En línea]. Available: https://datos.gob.es/es/blog/la-importancia-de-la-anonimizacion-y-la-privacidad-de-datos. [Último acceso: 28 03 2022].

[24] Agencia Española de Protección de Datos, «La K-Anonimidad como medidad de Privacidad,» de *Unidad de Evaluación y Estudios Tecnológicos*, Madrid, 2019.

[25] IBM, «Identificación y Autorización,» IBM MQ, [En línea]. Available: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm. [Último acceso: 10 05 2022].

[26] I. B. González, «HuMI: Plataforma para la Adquisición y Modelado de Señales de Interacción Hombre-Máquina,» UNIVERSIDAD AUTÓNOMA DE MADRID, Madrid, 2020.

[27] R. Gafni y I. Nagar, «Seguridad que afecta la experiencia del usuario,» Israel, 2016.

[28] Ministerio de Telecomunicaciones y de la Sociedad de la Información, «Subsecretaría de Gobierno Electrónico,» 10 2018. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Desarrollo-de-Gobierno-Electr%C3%B3nico-en-la-Administraci%C3%B3n-P%C3%BAblica-de-Ecuador-1.pdf. [Último acceso: 15 07 2022].

[29] Unión Europea, «REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO,» 04 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504. [Último acceso: 19 07 2022].

[30] M. A. González, «Primicias,» 03 12 2015. [En línea]. Available: https://www.primicias.ec/noticias/sociedad/cuatro-delitos-emision-carnes-discapacidad-fraudulentos/. [Último acceso: 01 08 2022].

[31] Subsecretaría de Gobierno Electrónico, «DESARROLLO DE GOBIERNO ELECTRÓNICO EN LA ADMINISTRACIÓN PÚBLICA DE ECUADOR,» 10 2018. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Desarrollo-de-Gobierno-Electr%C3%B3nico-en-la-Administraci%C3%B3n-P%C3%BAblica-de-Ecuador-1.pdf). [Último acceso: 01 08 2022].

[32] PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA, «DECLARA POLITICA DE ESTADO, LA MEJORA Y SIMPLIFICACION DE TRAMITES.,» 04 05 2018. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/Decreto-Ejecutivo-372.pdf. [Último acceso: 17 07 2022].

[33] Ministerio de Telecomunicaciones y de la Sociedad de la Información, «Plan Nacional de Gobierno Electrónico 2018-2021,» 2018. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf. [Último acceso: 15 07 2022].

[34] Ministerio de Telecomunicaciones y de la Sociedad de la Información, Informe de Rendición de Cuentas, 2020.

[35] Organización de Naciones Unidas, «Encuesta de gobierno electrónico de la ONU de 2020 (informe completo),» 2020. [En línea]. Available: https://desapublications.un.org/file/781. [Último acceso: 12 07 2022].

[36] Organización de Naciones Unidas, «ENCUESTAS DE GOBIERNO ELECTRÓNICO DE LA ONU,» 2020. [En línea]. Available: https://publicadministration.un.org/en/Research/UN-e-Government-Surveys. [Último acceso: 16 07 2022].

[37] Subsecretaría de Gobierno Electrónico, «Ecuador escala posiciones en el ranking mundial sobre el desarrollo del Gobierno Electrónico,» 2020. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/ecuador-escala-posiciones-en-el-ranking-mundial-sobre-el-desarrollo-del-gobierno-electronico/. [Último acceso: 16 07 2022].

[38] M. S. Troya, «La Ley de Transparencia no es la panacea de lucha contra la corrupción,» El País, 14 05 2013. [En línea]. Available: https://elpais.com/politica/2013/05/14/actualidad/1368526514_140115.html. [Último acceso: 17 07 2022].

[39] Global Right to Information Rating, «Mapa de calificación global del derecho a la información,» 17 07 2022. [En línea]. Available: https://www.rti-rating.org/. [Último acceso: 17 07 2022].

[40] Asamblea Nacional del Ecuador, «Ley de comercio electrónico, firmas y mensajes de datos,» 17 04 2002. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf. [Último acceso: 26 07 2022].

[41] EcuadorLegalOnline, «EcuadorLegalOnline,» 2022. [En línea]. Available: http://www.ecuadorlegalonline.com/. [Último acceso: 26 07 2022].

[42] Ecuador Web, «EcuadorWeb,» 2022. [En línea]. Available: https://ecuadorweb.net/. [Último acceso: 26 07 2022].

[43] Elvis Fernando, «Consultas Ecuador,» 2022. [En línea]. Available: https://play.google.com/store/apps/details?id=ec.consultasecuador.app&hl=es_EC&gl=US. [Último acceso: 26 07 2022].

[44] DatosMacro, «Ecuador: Economía y demografía,» 08 2022. [En línea]. Available: https://datosmacro.expansion.com/paises/ecuador. [Último acceso: 25 08 2022].

[45] Ministerio de Inclusión Económica y Social, «Plan de protección integral de la niñez y adolescencia al 2030,» 05 2021. [En línea]. Available: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2021/05/plan2030_ninez_version_consulta_compressed.pdf. [Último acceso: 25 08 2022].

[46] Consejo Nacional para la Igualdad de Discapacidades, «Estadísticas de Discapacidad,» 25 08 2022. [En línea]. Available: https://www.consejodiscapacidades.gob.ec/estadisticas-de-discapacidad/. [Último acceso: 25 08 2022].

[47] W. Torres, «Primicias,» 21 02 2022. [En línea]. Available: https://www.primicias.ec/noticias/economia/gobierno-desvinculacion-funcionarios-ahorro-ecuador/. [Último acceso: 25 08 2022].

[48] Ministerio de Gobierno, «Ministerio de Gobierno,» 2019. [En línea]. Available: https://www.ministeriodegobierno.gob.ec/la-policia-nacional-ahora-cuenta-con-mas-de-50-000-efectivos/. [Último acceso: 25 08 2022].

[49] Wikipedia, «Fuerzas Armadas del Ecuador,» 2022. [En línea]. Available: https://es.wikipedia.org/wiki/Fuerzas_Armadas_del_Ecuador#:~:text=La%20Fuerza%20Terrestre%2C%20m%C3%A1s%20conocida,miembros%20activos%20y%20170.000%20reservistas.. [Último acceso: 25 08 2022].

5. ANEXOS

ANEXO I. Dataset de sistemas de consulta pública

ANEXO II. Dataset de datos personales producto de la LOTAIP

ANEXO III. Tabla resumen de datos personales por categorías producto de la LOTAIP

ANEXO IV. Tabla de entidades públicas por categorías de datos personales de los sistemas de consulta pública

ANEXO I. Dataset de sistemas de consulta pública

N	Código	Nombre	Descripción	URL	CAPTCHA	Vulnerable a ataques	Protección Privacidad
1	AMT-1	Agencia Metropolitana de Tránsito	Consulta revisión técnica vehicular/impuesto al rodaje	http://servicios.amt.gob.ec:10444/appValoresPagarSAO/indexMain.jsp	✗	✗	✗
2	AMT-2	Agencia Metropolitana de Tránsito	Consulta de infracciones	https://servicios.axiscloud.ec/ConsultaInfracciones/paginas/ConsultaInfracciones.jsp?PS_EMPRESA=03	✗	✗	✗
3	AMT-3	Agencia Metropolitana de Tránsito	Historial de revisión técnica vehicular	http://servicios.aMTRA.gob.ec/web/historialRtv/#/hoMEDU	✗	✗	✓
4	ANT-1	Agencia Nacional de Tránsito	Consulta de citaciones	https://consultaweb.ant.gob.ec/PortalWEB/paginas/clientes/clp_criterio_consulta.jsp	✓	✗	✗
5	ANT-2	Agencia Nacional de Tránsito	Licencias	https://consultaweb.ant.gob.ec/SVT/paginas/portal/svf_solicitar_servicio.jsp?ps_param_tip_serv=LIC	✓	✗	✗
6	ANT-3	Agencia Nacional de Tránsito	Certificados de contuctor y vehículo	https://consultaweb.ant.gob.ec/SVT/paginas/portal/svf_solicitar_servicio.jsp?ps_param_tip_serv=CER	✗	✗	✗
7	ANT-4	Agencia Nacional de Tránsito	Consulta de puntos de licencia de conducir	https://ant.com.ec/licencias/consultar	✓	✗	✗
8	AME-1	Asociación de Municipalidades Ecuatorianas	Consulta de vehículos	https://www.consultavehicular.ame.gob.ec/consultas/	✗	✗	✗
9	CJ-1	Consejo de la Judicatura	Consulta de pensión alimenticia	http://supa.funcionjudicial.gob.ec/pensiones/publico/consulta.jsf	✗	✗	✗
10	CJ-2	Consejo de la Judicatura	Consulta de peritos	https://appsj.funcionjudicial.gob.ec/perito-web/pages/peritos_nacional.jsf	✗	✓	✗
11	CJ-3	Consejo de la Judicatura	Verificación de actos notariales	http://notarias.funcionjudicial.gob.ec/notarial/public/verificacionActo.jsf	✓	✗	✗
12	CJ-4	Consejo de la Judicatura	Consulta de información judicial individual	http://consultas.funcionjudicial.gob.ec/informacionjudicialindividual/pages/index.jsf#!/	✗	✗	✗
13	CJ-5	Consejo de la Judicatura	Consulta de procesos	http://consultas.funcionjudicial.gob.ec/informacionjudicial/public/informacion.jsf	✗	✗	✗
14	CGE-1	Contraloría General del Estado	Consulta declaraciones juradas	https://www.contraloria.gob.ec/Consultas/DeclaracionesJuradas	✓	✓	✓
15	CNT-1	Corporación Nacional de Telecomunicaciones	Guía telefónica	https://micnt.com.ec/cntapp/guia104/php/guia_cntat.php?hflagsubmit=0&cmbcriterio=1	✓	✗	✗
16	DNRP-1	Dirección Nacional de Registros Públicos	Datos de identidad	https://www.datosegura.gob.ec/web/guest/registro-web	✗	✗	✗
17	FGE-1	Fiscalía General del Estado	Consulta de actos administrativos	https://www.fiscalia.gob.ec/consulta-de-actos-administrativos/	✗	✓	✗
18	FGE-2	Fiscalía General del Estado	Consulta de delitos	https://www.fiscalia.gob.ec/consulta-de-noticias-del-delito/	✗	✓	✗
19	IESS-1	Instituto Ecuatoriano de Seguridad Social	Certificado de afiliación	https://www.iess.gob.ec/afiliado-web/pages/opcionesGenerales/seleccionCertificadoDeAfiliacion.jsf	✓	✗	✗
20	IESS-2	Instituto Ecuatoriano de Seguridad Social	Certificado de obligaciones patronales	https://www.iess.gob.ec/empleador-web/pages/morapatronal/certificadoCumplimientoPublico.jsf	✗	✗	✗
21	IESS-3	Instituto Ecuatoriano de Seguridad Social	Certificado de empleador	https://app.iess.gob.ec/gestion-empleador-certificado-web/	✓	✗	✗
22	IESS-4	Instituto Ecuatoriano de Seguridad Social	Consultar turno	https://app.iess.gob.ec/iess-gestion-turnero-enlinea-web/pages/conTurnoOnline.jsf?faces-redirect=true	✗	✗	✗
23	MDEF-1	Ministerio de Defensa	Certificado de pertenecer a Fuerzas Armadas	https://sidehu.midena.gob.ec/certificados/nofa.action	✓	✗	✗
24	MEDU-1	Ministerio de Educación	Consulta de estudiantes sistema educativo fiscal	https://juntos.educacion.gob.ec/index.php/consulta-sierra/asignacion	✓	✓	✗
25	MEDU-2	Ministerio de Educación	Consulta títulos de bachiller	http://servicios.educacion.gob.ec/titulacion25-web/faces/paginas/consulta-titulos-refrendados.xhtml	✓	✓	✗
26	MGOB-1	Ministerio de Gobierno	Certificado de antecedentes penales	https://certificados.ministeriodegobierno.gob.ec/gestorcertificados/antecedentes/	✓	✗	✗
27	MGOB-2	Ministerio de Gobierno	Certificado de pertenecer a Policía Nacional	https://certificados.ministeriodegobierno.gob.ec/gestorcertificados/dnobaja/	✗	✗	✗
28	MGOB-3	Ministerio de Gobierno	Consulta de impedimentos de salir del país	https://simiec.migracion.gob.ec:7445/consultaImpedimentos/	✓	✗	✗
29	MGOB-4	Ministerio de Gobierno	Consulta de guardias de seguridad privados	https://sicosep.ministeriodegobierno.gob.ec/empresas/mdi/mdiq/mdi1	✗	✗	✗
30	MGOB-5	Ministerio de Gobierno	Certificado de acreditación de guardias	https://sicosep.ministeriodegobierno.gob.ec/empresas/mdi/mdiq/mdi6	✗	✗	✗
31	MIES-1	Ministerio de Inclusión Económica y Social	Consulta de registro social	https://siirs.registrosocial.gob.ec/pages/publico/busquedaPublica.jsf	✓	✗	✓
32	MIES-2	Ministerio de Inclusión Económica y Social	Generación de trámites	https://tramitesenlinea.inclusion.gob.ec/tramiteonl/views/public/registro_inicio.jsf	✓	✗	✗
33	MIES-3	Ministerio de Inclusión Económica y Social	Consulta de usuarios de bonos y pensiones	https://siimiesalpha.inclusion.gob.ec/emergente/views/public/pageConsultaNuevoBeneficiario.jsf	✓	✗	✗
34	MSP-1	Ministerio de Salud Pública	Consulta de cobertura de salud	https://coresalud.msp.gob.ec/coresalud/app.php/publico/rpis/afiliacion/consulta	✓	✗	✗
35	MSP-2	Ministerio de Salud Pública	Certificado de vacunación	https://certificados-vacunas.msp.gob.ec/	✓	✗	✗
36	MTRA-1	Ministerio del Trabajo	Consulta de dependencia laboral	https://dependenciasectorpublico.trabajo.gob.ec/DependenciaLaboralSectorPublico/index.xhtml	✗	✗	✗
37	MTRA-2	Ministerio del Trabajo	Buscar impedimento trabajo	https://certificadoimpedimento.trabajo.gob.ec/BusquedaImpedido/	✗	✗	✗
38	MUNUIO-1	Municipio de Quito	Consulta de obligaciones	https://pam.quito.gob.ec/ConsultadeImpuestos/	✓	✗	✓
39	MUNUIO-2	Municipio de Quito	Consulta predio - IRM	https://pam.quito.gob.ec/mdmq_web_irm/irm/buscarPredio.jsf	✓	✗	✗
40	MUNUIO-3	Municipio de Quito	Sistema de reserva de turnos	http://turnosecuador.com/mdmq/	✗	✗	✗
41	REGCIV-1	Registro Civil	Consulta de informes estadístico de nacido vivo	http://servicios1.registrocivil.gob.ec/revit/consultaCiudadana.jsf#_	✓	✗	✗
42	REGCIV-2	Registro Civil	Consulta de datos	https://www.corporacionregistrocivil.gob.ec/pages/CeduladosGratuita.aspx	✓	✗	✗
43	SENESCYT-1	Secretaría Nacional de Educación Superior	Consulta de títulos registrados	https://www.senescyt.gob.ec/consulta-titulos-web/faces/vista/consulta/consulta.xhtml;jsessionid=ESw0CC9niZqT9f3iz5D8qlip.d28f0bce-6f01-372b-b0a2-648dc7d61c7b	✗	✓	✗
44	SENESCYT-2	Secretaría Nacional de Educación Superior	Consulta de estado de títulos extranjeros	https://www.senescyt.gob.ec/consulta-titulos-web/faces/vista/consulta/consultaEstadoExtranjero.xhtml	✗	✗	✗
45	SENESCYT-3	Secretaría Nacional de Educación Superior	Certificado de ser o no becario	https://www.senescyt.gob.ec/certificadoBecas/faces/consulta.xhtml	✗	✗	✗
46	SENESCYT-4	Secretaría Nacional de Educación Superior	Certificado de crédito educativo	https://www.senescyt.gob.ec/FormulariosAPP/faces/consulta_certificado.xhtml	✗	✗	✗
47	SENESCYT-5	Secretaría Nacional de Educación Superior	Consulta de becarios	https://www.senescyt.gob.ec/CompensacionApp/faces/seguimiento_ocupacional_user.xhtml	✗	✗	✗
48	SRI-1	Servicio de Rentas Internas	Consulta de RUC	https://srienlinea.sri.gob.ec/sri-en-linea/SriRucWeb/ConsultaRuc/Consultas/consultaRuc	✓	✓	✗
49	SRI-2	Servicio de Rentas Internas	Consulta valores a pagar por placa o chasis	https://srienlinea.sri.gob.ec/sri-en-linea/SriVehiculosWeb/ConsultaValoresPagarVehiculo/Consultas/consultaRubros	✓	✗	✗
50	SRI-3	Servicio de Rentas Internas	Consulta de estado tributario	https://srienlinea.sri.gob.ec/sri-en-linea/SriDeclaracionesWeb/EstadoTributario/Consultas/consultaEstadoTributario	✓	✗	✗
51	SRI-4	Servicio de Rentas Internas	Consulta de contribuyentes	https://srienlinea.sri.gob.ec/sri-en-linea/SriPagosWeb/ConsultaDeudasFirmesImpugnadas/Consultas/consultaDeudasFirmesImpugnadas	✓	✓	✗
52	SRI-5	Servicio de Rentas Internas	Consulta de impuesto a la renta y salida de divisas	https://srienlinea.sri.gob.ec/sri-en-linea/SriDeclaracionesWeb/ConsultaImpuestoRenta/Consultas/consultaImpuestoRenta	✓	✓	✗
53	SRI-6	Servicio de Rentas Internas	Consulta de ranking de deudas	https://srienlinea.sri.gob.ec/sri-en-linea/SriPagosWeb/ConsultaRankingDeudas/Consultas/mostrarRankingDeudas	✓	✓	✗
54	SRI-7	Servicio de Rentas Internas	Consulta de herencias/legados	https://srienlinea.sri.gob.ec/sri-en-linea/SriDeclaracionesWeb/ConsultaHerencia/Consultas/mostraREGCIVonsultaHerencia	✓	✗	✗
55	SRI-8	Servicio de Rentas Internas	Consulta de citas previas	https://srienlinea.sri.gob.ec/turnos-internet-web/publico/consultaAnulaCita.jsf?pathMPT=Cita%20previa&actualMPT=Consultar%2Fanular%20cita%20previa	✓	✗	✗
56	SRI-9	Servicio de Rentas Internas	Consultar reporte de pagos	https://srienlinea.sri.gob.ec/sri-en-linea/SriVehiculosWeb/ReportePagosVehiculo/Consultas/consultarPagos	✓	✗	✗
57	SRI-10	Servicio de Rentas Internas	Consultar información del contribuyente	https://srienlinea.sri.gob.ec/sri-en-linea/SriDeclaracionesWeb/ConsultaImpuestoRenta/Consultas/consultaImpuestoRenta	✓	✓	✗
58	SENAE-1	Servicio Nacional de Aduana del Ecuador	Consulta de registro consular	https://www.aduana.gob.ec/consultacupos/	✗	✗	✗
59	SENAE-2	Servicio Nacional de Aduana del Ecuador	Consulta de clasificación	https://www.aduana.gob.ec/consulta-de-clasificacion/	✗	✓	✗
60	SENAE-3	Servicio Nacional de Aduana del Ecuador	Consulta de certificado de cumplimiento	https://www.aduana.gob.ec/consulta-de-certificado-cumplimiento/	✗	✗	✗
61	SENAE-4	Servicio Nacional de Aduana del Ecuador	Consulta de grado de discapacidad	https://servicios.aduana.gob.ec/servicios/ui/consulta-grado-discapacidad.xhtml	✗	✗	✗
62	SUPERCIAS-1	Superintendencia de Compañías	Consulta de personas	https://appscvs1.supercias.gob.ec/consultaPersona/consulta_cia_param.zul	✗	✓	✗
63	SUPERCIAS-2	Superintendencia de Compañías	Consulta de credenciales seguros	https://seguros.supercias.gob.ec/SolicitudesCalificacionAsesores/buscarCredencialPublicada.zul	✗	✓	✗
64	SUPERCIAS-3	Superintendencia de Compañías	Certificado de accionista	https://appscvs1.supercias.gob.ec/consultaPersona/consulta_noacc_param.zul	✗	✓	✗

ANEXO II. **Dataset de datos personales producto de la LOTAIP**

Literal	Ítem de dato personal	Dato Personal	Categoría	Sensible
b1	Puesto institucional	Cargo sector público	Laboral	✗
b1	Dirección de correo electrónico	Dirección de correo electrónico	Identificador	✗
b1	Unidad laboral	Lugar de trabajo	Demográfico	✗
b1	Nombres completos	Nombres completos	Identificador	✗
b1	Teléfono institucional	Número de teléfono	Ubicación	✗
b1	Dirección de trabajo	Ubicación geográfica	Ubicación	✗
b2	Puesto institucional	Cargo sector público	Laboral	✗
b2	Unidad laboral	Lugar de trabajo	Demográfico	✗
b2	Nombres completos	Nombres completos	Identificador	✗
c	Puesto institucional	Cargo sector público	Laboral	✗
c	Grado o escala de jerarquía de puesto	Grado de jerarquía de puesto	Laboral	✗
c	Remuneración mensual	Ingresos	Patrimonio	✗
c	Remuneración anual	Ingresos	Patrimonio	✗
c	Décimo tercera remuneración	Ingresos	Patrimonio	✗
c	Décima cuarta remuneración	Ingresos	Patrimonio	✗
c	Horas suplementarias y extraordinarias	Ingresos	Patrimonio	✗
c	Encargos y subrogaciones	Ingresos	Patrimonio	✗
c	Total ingresos adicionales	Ingresos	Patrimonio	✗
c	Nombres completos	Nombres completos	Identificador	✗
c	Número de partida presupuestaria	Número de partida presupuestaria	Identificador	✗
c	Régimen laboral	Régimen laboral	Laboral	✗
j	Objeto de contrato	Detalles de contrato	Laboral	✗
j	Tipo de contrato	Detalles de contrato	Laboral	✗
j	Monto de deuda	Deuda	Patrimonio	✗
j	Estatus de apelación de contratista	Estatus apelación	Judicial	✗
j	Identificador tributario de contribuyente	Identificador tributario de contribuyente	Identificador	✗
j	Nombres completos	Nombres completos	Identificador	✗
j	Causas de incumplimiento	Procesos judiciales/infracciones	Judicial	✓
n	Puesto institucional	Cargo sector público	Laboral	✗
n	Detalles de viaje	Detalles de viaje	Laboral	✗
n	Fecha de viaje	Fecha de viaje	Ubicación	✗
n	Valor de viático	Ingresos	Patrimonio	✗
n	Nombres completos	Nombres completos	Identificador	✗

ANEXO III. **Tabla resumen de datos personales por categorías producto de la LOTAIP**

Categoría	Dato Personal
Identificador	Dirección de correo electrónico
	Identificador tributario de contribuyente
	Nombres completos
	Número de partida presupuestaria
Demográfico	Lugar de trabajo
Laboral	Cargo sector público
	Detalles de contrato
	Detalles de viaje
	Grado de jerarquía de puesto
	Régimen laboral
Patrimonio	Deuda
	Ingresos
Judicial	Estatus apelación
	Procesos judiciales/infracciones
Ubicación	Fecha de viaje
	Número de teléfono
	Ubicación geográfica

ANEXO IV. Tabla de entidades públicas por categorías de datos personales de los sistemas de consulta pública

				I	QI			C				C/CE			
#	Logo	Entidad	Porcentaje de datos personales revelados	Identificador	Demográfico	Educación	Laboral	Ubicación	Judiciales	Patrimonio	Confidencial	Salud	Sensibles	De niñas, niños y adolescentes	De personas con discapacidad
1		Ministerio de Gobierno	62%	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗
2		Fiscalía General del Estado	54%	✓	✓	✗	✗	✓	✓	✗	✗	✓	✓	✗	✓
3		Registro Civil	54%	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗
4		Servicio de Rentas Internas	54%	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✗
5		Ministerio de Educación	46%	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗
6		Ministerio de Inclusión Económica y Social	46%	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	✓
7		Consejo de la Judicatura	46%	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗
8		Secretaría Nacional de Educación Superior	46%	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗
9		Servicio Nacional de Aduana del Ecuador	46%	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓
10		Superintendencia de Compañías	46%	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗
11		Contraloría General del Estado	38%	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
12		Agencia Nacional de Tránsito	38%	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✗	✗
13		Instituto Ecuatoriano de Seguridad Social	38%	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗
14		Ministerio de Salud Pública	38%	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗
15		Ministerio del Trabajo	23%	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
16		Municipio de Quito	23%	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
17		Agencia Metropolitana de Tránsito	15%	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
18		Asociación de Municipalidades Ecuatorianas	15%	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
19		Corporación Nacional de Telecomunicaciones	15%	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
20		Ministerio de Defensa	15%	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
21		Dirección Nacional de Registros Públicos	8%	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
			Porcentaje de instituciones que revelan datos personales	100%	62%	24%	38%	57%	24%	48%	5%	33%	52%	19%	14%