UNIVERSIDAD ESTATAL DE BOLÍVAR

Facultad de Jurisprudencia Ciencias Sociales y Políticas

Carrera de Derecho

Trabajo de Integración Curricular Modalidad Proyecto de Investigación Previo la obtención del Título de Abogada

Tema:

Tecnologías de control biométrico en el empleo público ecuatoriano: vigilancia institucional, poder administrativo y derechos humanos

Autora

Fernanda Mishel Guacho Auquilla

Tutor

Dr. Ángel Teodoro Naranjo Estrada

Guaranda - Ecuador

2026

CERTIFICADO DE APROBACION

Yo, **Doctor Ángel Teodoro Naranjo Estrada** en mi calidad de Tutor del Proyecto de Investigación, designado por disposición de Consejo Directivo, bajo juramento **CERTIFICO:** que la señorita **Fernanda Mishel Guacho Auquilla,** egresada de la Universidad Estatal de Bolívar, Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Derecho, ha cumplido con su trabajo de grado previo a la obtención del título de Abogada; con el tema: **"TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS";** mismo que ha cumplido con todos los requerimientos exigidos por la institución, por lo que se aprueba la misma.

Es todo cuanto puedo decir en honor a la verdad, facultando a la interesada a hacer uso de la presente, así como también se autoriza la presentación para la calificación por parte del jurado respectivo.

Atentamente,



Dr. Ángel Naranjo Estrada
Tutor

DECLARACIÓN JURAMENTADA DE AUTENTICIDAD DE AUTORÍA

Yo; **FERNANDA MISHEL GUACHO AUQUILLA**, egresada de la Carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, bajo juramento declaro en forma libre y voluntaria que el presente Proyecto, con el tema: **"TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS";** es de mí autoría, así como las expresiones vertidas en la misma, que se ha realizado bajo la recopilación bibliográfica tanto de libros, revistas, publicaciones, así como de artículos de la legislación ecuatoriana para el presente trabajo investigativo.

Atentamente,

Fernanda Mishel Guacho Auquilla
Autora

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

Notaria Tercera del Cantón Guaranda
Msc.Ab. Henry Rojas Narvaez
Notario

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

No. ESCRITURA	20260201003P01897

DECLARACION JURAMENTADA
OTORGADA POR:
GUACHO AUQUILLA FERNANDA MISHEL
CUANTIA: INDETERMINADA
FACTURA: 001-003-000000614
DI: 2 COPIAS

En la ciudad de Guaranda, capital de la provincia Bolívar, República del Ecuador, hoy día dieciséis de junio de dos mil veintiséis, **ante mi Abogado HENRY ROJAS NARVAEZ, Notario Público Tercero del Cantón Guaranda**, comparece sin coacción ni amenaza de ninguna naturaleza la señorita: **GUACHO AUQUILLA FERNANDA MISHEL** estado civil soltera, domiciliada en Riobamba y de paso por este cantón de Guaranda, provincia de Bolívar, con celular número 0987883551, por sus propios derechos. La compareciente es de nacionalidad ecuatoriana, mayor de edad, hábil e idónea para contratar y obligarse a quien de conocerla doy fe en virtud de haberme exhibido sus documentos de identificación y con su autorización se ha procedido a verificar la información en el Sistema Nacional de Identificación Ciudadana, además autoriza el tratamiento de sus datos personales en este protocolo, bien instruido por mí el Notario con el objeto y resultado de esta escritura pública a la que procede libre y voluntariamente, advertida de la gravedad del juramento y las penas de perjurio, me presenta su declaración Bajo Juramento que dice: Declaro que el presente trabajo de investigación titulado: **"TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO; VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS".** Previo la obtención del título de Abogada, de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, es de mí exclusiva autoría, este documento no ha sido previamente presentado por ningún grado de calificación profesional y que las referencias bibliográficas que se incluyen han sido consultadas por la autora. Es todo cuanto puedo declarar en honor a la verdad, la misma que la hago para los fines legales pertinentes. **HASTA AQUÍ LA DECLARACIÓN JURADA.** La misma que queda elevada a escritura pública con todo su valor legal. Para el otorgamiento de la presente escritura pública se observaron todos los preceptos legales del caso, leída que le fue al compareciente por mí el Notario en unidad de acto, aquel se afirma y se ratifica de todo lo expuesto y firma conmigo en unidad de acto, quedando incorporado al protocolo de esta Notaria, la presente declaración, de todo lo cual doy fe.-

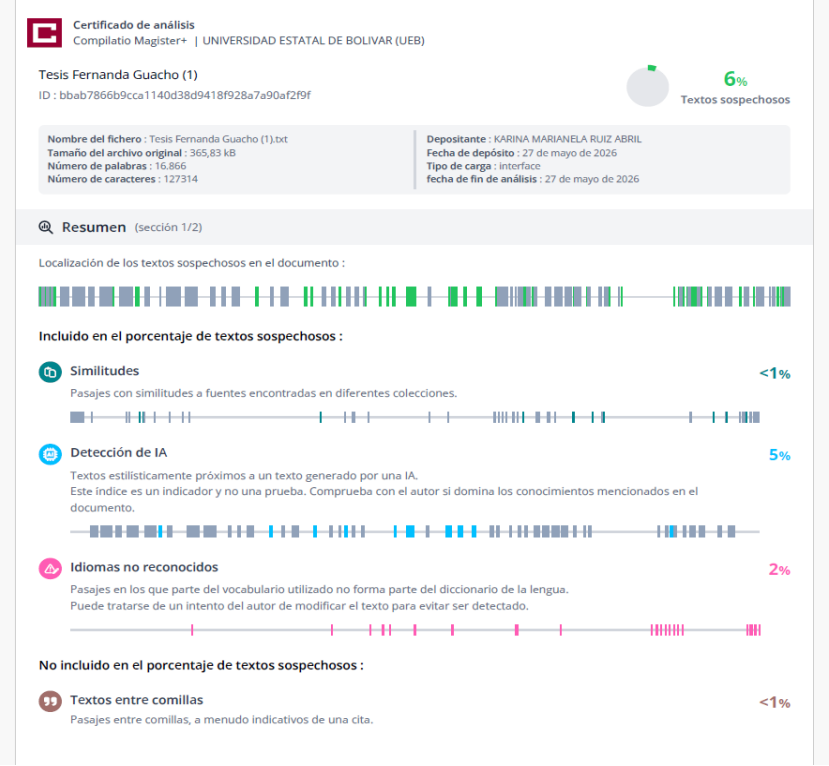
GUACHO AUQUILLA FERNANDA MISHEL
C.C. 0650036452

AB. HENRY ROJAS NARVAEZ
NOTARIO TERCERO DEL CANTON GUARANDA

INFORME CERTIFICADO

EN CALIDAD DE DOCENTE TUTOR DE LA UNIVERSIDAD ESTATAL DE BOLIVAR CERTIFICO QUE:

Fernanda Mishel Guacho Auquilla con el trabajo titulado "TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS", ha enviado concluido el mentado trabajo por el "servicio de análisis documental de COPILATION 6%" de similitud llegando dicho análisis al correo del compareciente en calidad de Docente – Tutor y orientador en el proceso, al tenor de lo prescrito por el reglamento correspondiente.



Certificado de análisis
Compilatio Magister+ | UNIVERSIDAD ESTATAL DE BOLIVAR (UEB)

Tesis Fernanda Guacho (1)
ID : bbab7866b9cca1140d38d9418f928a7a90af2f9f

6%
Textos sospechosos

Nombre del fichero : Tesis Fernanda Guacho (1).txt
Tamaño del archivo original : 365,83 kB
Número de palabras : 16.866
Número de caracteres : 127314

Depositante : KARINA MARIANELA RUIZ ABRIL
Fecha de depósito : 27 de mayo de 2026
Tipo de carga : interface
fecha de fin de análisis : 27 de mayo de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes <1%
Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

Detección de IA 5%
Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos 2%
Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas <1%
Pasajes entre comillas, a menudo indicativos de una cita.

Particular que certifico para los fines reglamentarios correspondientes.

Guaranda 12 de junio de 2026

Dr. Angel Naranjo Estrada
Tutor



Particular que certifico para los fines reglamentarios correspondientes.

Guaranda 12 de junio de 2026

Dr. Ángel Naranjo Estrada
Tutor

DERECHOS DE AUTOR

Yo: Fernanda Mishel Guacho Auquilla, portador de la Cédula de Identidad No **0650036452,** en calidad de autor titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Tema: Tecnologías de control biométrico en el empleo público ecuatoriano: vigilancia institucional, poder administrativo y derechos humanos,** modalidad Proyecto de Investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.



Fernanda Mishel Guacho Auquilla

Autora

DEDICATORIA

Llegar a la meta de este gran sueño no es un triunfo que me pertenezca únicamente; es la suma de cada gesto de amor, de cada abrazo sincero y apoyo incondicional de quienes han caminado a mi lado.

Asi mismo dedico este trabajo a mi bisabuelito, José Taco, por su cariño incondicional y por ser esa guía firme que me acompañó durante todo este camino, honrando con amor la memoria de mis abuelitos maternos, Luis Auquilla y Gloria Guzmán.

A mi madre, Norma Auquilla, ejemplo vivo de fortaleza, valentía y perseverancia. Tu entrega incansable y tu fe inquebrantable en mí han sido la luz en los momentos de duda, por ser mi refugio, mi inspiración y la razón más profunda de este sueño alcanzado.

A mis hermanos, Melany por ser ese lazo inquebrantable que me recordó siempre de dónde vengo y hacia dónde voy, Luis cuya presencia ha sido una motivación constante, un ejemplo silencioso de perseverancia que me enseñó a no rendirme.

A Félix, por haberte convertido en ese refugio al que siempre supe que podía volver, incluso cuando todo dentro de mí parecía desordenarse, por caminar a mi lado sin prisa, entendiendo mis silencios, mis dudas y mis caídas, por sostenerme no solo con palabras, sino con gestos, con presencia, y con esa forma tan tuya de permanecer

A mi padre, Alfonso Guacho, aunque ya no puedo escuchar su voz ni sentir su abrazo, sé que desde el cielo, sigue guiando mi camino con ese amor silencioso que nunca se apaga, acompañándome en cada decisión, en cada caída y en cada logro alcanzado.

A mis pequeños pero grandes amigos Theo, Tommi, Zeus, y Rocky por ser mis compañeros de desvelo y cuya luz continúa iluminando mi vida.

A mi familia materna, por su apoyo constante y sus palabras llenas de sabiduría; y a mi familia paterna, por su cariño sincero y por compartir conmigo la alegría de este logro.

Fernanda Mishel Guacho Auquilla

AGRADECIMIENTO

A Dios, a mi madre amada del Cisne y del Carmen, y a mi patrono San José, por ser esa presencia sagrada que, aun en silencio, sostuvo mi camino con fe amor y sabiduría cuando más lo necesité, ustedes, mis santitos, que nunca me soltaron, incluso en los días en que mis fuerzas se apagaban y mi esperanza parecía desvanecerse.

A mi familia, de manera especial a mi madre Norma Auquilla, aunque este proceso me exigió estar lejos de ustedes, su apoyo moral, su ejemplo de trabajo y su cariño incondicional acortaron cualquier distancia. Gracias por creer en mí; fue ese respaldo desde la distancia el que me dio el impulso definitivo para no rendirme y alcanzar esta meta.

A la Universidad Estatal de Bolívar, por abrirme sus puertas y confiar en mi formación. Expreso mi gratitud a la institución y a mis docentes por brindarme los conocimientos, el espacio y las herramientas académicas que hicieron posible la materialización de esta investigación.

Fernanda Mishel Guacho Auquilla

INDICE

CERTIFICADO DE APROBACION I

DECLARACIÓN JURAMENTADA DE AUTENTICIDAD DE AUTORÍA II

INFORME CERTIFICADO IV

DEDICATORIA IV

AGRADECIMIENTO V

CAPITULO I: PROBLEMA 1

1. Titulo: 1

1.1 Resumen 2

Abstrac 4

Tukuy yuyay 6

1.2 Introducción 8

1.3 Planteamiento Del Problema 10

1.4 Formulación del Problema 11

1.5 Hipótesis 11

1.6 Variables 11

1.6.1 Variable Independiente 11

1.7 Objetivos 11

1.7.1 Objetivo General 11

1.7.2 Objetivos Específicos 12

1.8 Justificación 12

CAP II MARCO TEÓRICO 14

UNIDAD I Regulación del uso y control biométrico en el empleo público 14

Triada normativa, Constitución LOSEP Código Administrativo 14

Unidad II Conflicto Real Entre Normativas Ecuatorianas 18

UNIDAD III Riesgos jurídicos del tratamiento de datos biométricos en el empleo público 30

Unidad IV Derecho Comparado 34

CAPÍTULO III: MARCO METODOLÓGICO 41
3 MÉTODO DE INVESTIGACIÓN 41
3.1 Tipo de Investigación 41
3.2 Técnicas e instrumentos de investigación 41
3.3 Criterio de Inclusión y Criterio De Exclusión 42
3.4 Unidades de Análisis (Población y Muestra) 42
3.5 Localización geográfica de estudio 42
1. Capítulo IV: Resultados y Discusión 43
4. Resultados 43
4.1 Discusión 59
Capitulo V- Conclusiones y Recomendaciones 61
5.1 Conclusiones 61
5.2 Recomendaciones 62
ANEXOS 1
ANEXOS 3
EVIDENCIAS 4
ENTREVISTA 6

INIDICE DE TABLAS

Tabla 1……43
Tabla 2……45
Tabla 3……47
Tabla 4……48
Tabla 5……49
Tabla 6……51
Tabla 7……53
Tabla 8……54
Tabla 9……55
Tabla 10……..56
Tabla 11……..57
Tabla 12……..58

CAPITULO I: PROBLEMA

1. **Titulo:**

   "TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS"

1.1 Resumen

El control biométrico en el empleo público ecuatoriano se ha convertido en una práctica extendida dentro de las instituciones del Estado, implementada como mecanismo de verificación de asistencia y vigilancia institucional. Sin embargo, su aplicación ha ocurrido al margen de un análisis jurídico riguroso, sin que las entidades responsables hayan verificado su compatibilidad con el marco normativo vigente ni garantizado la protección efectiva de los derechos de los servidores públicos.

El problema central que esta investigación identifica es que la Ley Orgánica de Protección de Datos Personales del Ecuador, vigente desde 2021, no establece disposiciones específicas sobre el tratamiento, conservación y eliminación de datos biométricos en el contexto del empleo público. Esta omisión genera un vacío normativo que impide determinar con precisión a qué institución le corresponde eliminar esos datos una vez que la relación laboral ha concluido, bajo qué condiciones pueden ser conservados durante su vigencia y qué mecanismos de control existen para prevenir su uso indebido. Ese vacío no es un detalle técnico menor: es la causa directa de que el poder administrativo del Estado, al ejercer sus facultades de vigilancia institucional a través de sistemas biométricos, opere sin límites jurídicos claramente definidos, lo que convierte esa vigilancia en una práctica potencialmente desproporcionada.

Esta situación vulnera derechos constitucionales reconocidos por la Constitución de la República del Ecuador de 2008: el derecho a la privacidad, el derecho a la intimidad personal y familiar, y el derecho a la autodeterminación informativa, todos ellos consagrados en el artículo 66 de la norma suprema. Adicionalmente, el principio de legalidad establecido en el artículo 226 de la Constitución exige que el Estado ejerza únicamente las competencias que le han sido expresamente atribuidas, condición que no se cumple cuando las instituciones públicas implementan sistemas biométricos sin una habilitación legal específica que lo autorice.

La investigación examina este problema desde cuatro dimensiones: el análisis del marco normativo ecuatoriano aplicable, la determinación de los límites constitucionales del poder administrativo de control y vigilancia laboral, la identificación de los riesgos jurídicos asociados al tratamiento de datos biométricos como datos sensibles, y el estudio del derecho comparado latinoamericano en países como Colombia, México y Brasil, de cuyas experiencias se extraen lineamientos regulatorios aplicables al contexto ecuatoriano. El objetivo final es demostrar que el vacío normativo existente no es una

situación tolerable bajo el ordenamiento jurídico ecuatoriano vigente, y que su corrección requiere una intervención normativa que conecte de manera expresa la LOSEP con la LOPDP, garantizando que la vigilancia institucional biométrica opere dentro de los límites que la Constitución y los derechos humanos de los servidores públicos imponen al Estado.

Palabras clave: control biométrico, empleo público, datos biométricos, vacío normativo, poder administrativo, autodeterminación informativa, privacidad, intimidad, proporcionalidad, derecho comparado, Ecuador.

Abstrac

Biometric control in Ecuadorian public employment has become a widespread practice within State institutions, implemented as a mechanism for attendance verification and institutional surveillance. However, its application has occurred without rigorous legal analysis, and without the responsible entities verifying its compatibility with the current regulatory framework or guaranteeing the effective protection of public servants' rights.

The central problem identified by this research is that the Organic Law on Personal Data Protection of Ecuador, in force since 2021, does not establish specific provisions regarding the processing, storage, and deletion of biometric data within the context of public employment. This omission creates a regulatory gap that prevents determining precisely which institution is responsible for deleting such data once the employment relationship has ended, under what conditions they may be retained during its validity, and what control mechanisms exist to prevent their misuse. This gap is not a minor technical issue: it is the direct cause of the State's administrative power, when exercising its institutional surveillance functions through biometric systems, operating without clearly defined legal limits, thus turning such surveillance into a potentially disproportionate practice.

This situation violates constitutional rights recognized by the 2008 Constitution of the Republic of Ecuador: the right to privacy, the right to personal and family intimacy, and the right to informational self-determination, all enshrined in Article 66 of the supreme law. Additionally, the principle of legality established in Article 226 of the Constitution requires that the State exercise only those powers expressly granted to it, a condition that is not fulfilled when public institutions implement biometric systems without specific legal authorization.

This research examines the problem from four dimensions: the analysis of the applicable Ecuadorian legal framework, the determination of the constitutional limits of administrative power in labor control and surveillance, the identification of legal risks associated with the processing of biometric data as sensitive data, and the study of comparative law in Latin American countries such as Colombia, Mexico, and Brazil, from whose experiences regulatory guidelines applicable to the Ecuadorian context are derived. The ultimate objective is to demonstrate that the existing regulatory gap is not tolerable under the current Ecuadorian legal system, and that its correction requires regulatory intervention that explicitly connects the LOSEP with the LOPDP, ensuring

that biometric institutional surveillance operates within the limits imposed by the Constitution and the human rights of public servants.

Keywords: biometric control, public employment, biometric data, regulatory gap, administrative power, informational self-determination, privacy, intimacy, proportionality, comparative law, Ecuador.

Tukuy yuyay

Ecuador llaktapi, kamachik runakunapak llamkaypi biométrico control nishka rurayka kunan punchakunapi ashka Estado ukupi llamkak wasikunapi yaykushka kan, asistencia rikuchinapak chaymanta institucionpi rikcharishka vigilancia ruraypak. Shinapash, kay rurayka mana sumak kamachik yuyaywan rikurishka, mana responsable entidades rikushka kanchu ima shinalla kay ruray kamachikkunawan tupakushka kan, nishpash mana garantizashka kanchu llamkak runakunapak derechokuna alli wakaychishka kan.

Kay yachaykuna rikuchishka hatun llakikuna kaymi: Ecuadorpi Ley Orgánica de Protección de Datos Personales, 2021 watamanta shamushka, mana churanchu ima shina biométrico datos tratamientota, wakaychayta, chinkachinata ima shina rurana kan llamkaypi público contexto ukupi. Kay mana churashka kamachikpi, huk vacío normativo tiyashka kan, mana allinta yachayta atipanchu ima institucion chay datos chinkachinata rikunata, ima shina wakaychana kan llamkaykuna purishkapi, chaymanta ima controlkuna tiyan mana alli ruranata harkanakapak. Kay vacío mana uchilla llaki kanchu: kaymi causa directa Estado poder administrativo, biométrico sistemakunawan vigilancia ruranapi, mana rikuchishka límitekunawan llamkashpa, chayrayku vigilancia desproporcionado kanman.

Kay ruraymi Constitución de la República del Ecuador 2008pi killkashka derechokunata paktachin: privacidad, intimidad personal y familiar, chaymanta autodeterminación informativa (artículo 66). Shinallata, principio de legalidad (artículo 226) nishka rikuchin Estado solo rurana kan imakuna kamachikpi killkashka kashkakunata, chay mana cumplinchu kunan biométrico sistemakunata mana legal autorizaciónwan rurashpa.

Kay yachayka rikun chusku rikuraykunamanta: Ecuador kamachik marco análisis, poder administrativo límite constitucional rikuray, biométrico datos riesgos jurídicos rikuchiy, chaymanta derecho comparado Latinoamérica llaktakunapi (Colombia, México, Brasil). Chay llaktakunamanta yachaykunata apamushka kan Ecuadorpi aplicanakapak.

Kay yachaypa tukuy yuyayka rikuchiymi: kay vacío normativo mana allikanchu Ecuador kamachikpi, shinallata arreglanapak munan huk reforma normativa, LOSEPwan LOPDPwan tinkuchishpa, biométrico vigilancia Estado ukupi Constituciónmanta derechokuna respetashpa rurana kan.

Palabrakuna clave: biométrico control, llamkay público, biométrico datos, vacío normativo, poder administrativo, autodeterminación informativa, privacidad, intimidad, proporcionalidad, derecho comparado, Ecuador.

1.2 Introducción

Con respecto a la transformación digital del estado, la implementación de tecnologías de control biométrico en el sector público ha adquirido una creciente relevancia, particularmente en ámbitos como el control de asistencia laboral, la identificación de servidores públicos y el acceso a instalaciones institucionales. Estas herramientas, basadas en el reconocimiento de características físicas únicas como la huella digital, el reconocimiento facial o el escaneo de iris, prometen mejorar la eficiencia administrativa y fortalecer los mecanismos de control institucional; sin embargo, su utilización plantea tensiones jurídicas significativas en relación con la protección de los derechos humanos, especialmente a partir de la vigencia de la Ley Orgánica de Protección de Datos Personales desde el año 2021.

Este conflicto ocurre cada mañana, en cientos de instituciones públicas ecuatorianas, cuando un servidor extiende su dedo hacia un lector biométrico sin saber con certeza quién custodia ese dato, durante cuánto tiempo lo conservará la institución, si será compartido con terceros, o qué ocurrirá con él cuando deje de prestar sus servicios. La respuesta a esas preguntas no está clara en el ordenamiento jurídico ecuatoriano actual, y esa falta de claridad es precisamente el problema que esta investigación busca examinar.

Ecuador cuenta desde el 26 de mayo de 2021 con la Ley Orgánica de Protección de Datos Personales, una norma que representó un avance significativo en la protección de los derechos digitales de los ciudadanos y que clasifica los datos biométricos como datos de categoría especial o datos sensibles, cuyo tratamiento está prohibido como regla general salvo que concurra alguna de las bases de legitimación taxativamente reconocidas en la norma. Sin embargo, esa misma ley no establece disposiciones específicas para el tratamiento, conservación y eliminación de datos biométricos en el marco del empleo público. La Ley Orgánica del Servicio Público, por su parte, define con claridad la obligación de los servidores de cumplir su jornada laboral, pero no establece qué métodos puede utilizar el Estado para verificar ese cumplimiento ni impone límites expresos al uso de tecnologías que impliquen el procesamiento de datos de categoría especial. El resultado de esa desconexión normativa es un vacío que las instituciones públicas han llenado con sus propias interpretaciones, implementando sistemas biométricos sin haber realizado evaluaciones de impacto previas, sin contar con bases de legitimación documentadas y sin ofrecer a sus servidores alternativas reales al uso de su información biométrica.

La magnitud de ese vacío se vuelve aún más evidente cuando se analiza la experiencia regional Colombia, México y Brasil países con marcos normativos de protección de datos más equilibrados que el ecuatoriano han enfrentado consecuencias graves derivadas precisamente de implementar tecnologías biométricas en el sector público sin las garantías jurídicas e institucionales adecuadas la mayor filtración de datos de la historia latinoamericana, que afectó a más de 220 millones de personas, ocurrió durante el período en que el país tenía una ley de protección de datos aprobada pero todavía no contaba con una autoridad operativa capaz de hacerla cumplir ecuador atraviesa hoy ese mismo período de transición y los riesgos son equivalentes.

En el plano constitucional, la tensión que genera el control biométrico en el empleo público no puede resolverse invocando únicamente la eficiencia administrativa la Constitución de la República del Ecuador de 2008 garantiza en su artículo 66 el derecho a la protección de datos personales, el derecho a la intimidad personal y familiar, y la prohibición de exigir o utilizar datos sensibles sin autorización del titular esos derechos no se suspenden cuando una persona ingresa al servicio público: son inalienables, irrenunciables e indivisibles conforme lo establece el artículo 11 de la propia Constitución.

La tecnología biométrica avanza a una velocidad que la regulación no ha podido seguir la norma de protección de datos existe, pero no se comunica adecuadamente con la normativa laboral pública. Y las instituciones implementan sistemas que afectan los derechos más íntimos de sus servidores sin que nadie les exija demostrar que esa implementación es jurídicamente legítima, proporcional y segura.

Frente a esa realidad, esta investigación se organiza en torno a cuatro objetivos específicos que buscan, en conjunto, ofrecer una comprensión integral del problema y una respuesta jurídica fundamentada. El primero examina el marco normativo ecuatoriano aplicable al control biométrico, identificando las disposiciones de la Constitución, la LOPDP y la LOSEP y las tensiones que entre ellas se generan. El segundo determina el alcance del poder administrativo del Estado en materia de control y vigilancia laboral, identificando sus límites constitucionales frente a los principios de legalidad y proporcionalidad. El tercero identifica los riesgos jurídicos específicos que el tratamiento de datos biométricos genera para los derechos a la privacidad, la intimidad y la autodeterminación informativa de los servidores públicos. Y el cuarto examina el derecho comparado latinoamericano, extrayendo de las experiencias de Colombia, México, Argentina y Brasil lineamientos regulatorios aplicables al contexto ecuatoriano

1.3 Planteamiento Del Problema

El uso de tecnologías de control biométrico en el empleo público como sistemas de reconocimiento facial, huella dactilar o escaneo de iris se ha expandido como mecanismo de control de asistencia, productividad y seguridad institucional. Pero hay que notar que su implementación en varias instituciones y en muchos casos, se lo ha hecho sin contar con un desarrollo normativo claro, integral y específico que regule adecuadamente el tratamiento de datos biométricos, los límites del poder administrativo y las garantías de los derechos fundamentales de los servidores públicos; más relevante aún sin tomar en cuenta disposiciones legales existentes como la Ley Orgánica de Protección de Datos Personales; norma promulgada en el año 2021 para fortalecer la seguridad y protección de datos personales de los ciudadanos en épocas de un acelerado avance tecnológico y los altos índices de inseguridad por los que atraviesa el estado ecuatoriano.

Esta situación genera tensiones entre la potestad de la administración pública para organizar, dirigir y controlar el servicio público, y los derechos constitucionales de los trabajadores, particularmente el derecho a la intimidad, a la protección de datos personales, a la dignidad humana y al consentimiento informado, reconocidos en la Constitución de la República del Ecuador de 2008 y en la Ley Orgánica de Protección de Datos Personales.

Es importante puntualizar que la utilización de tecnologías biométricas puede derivar en prácticas de vigilancia institucional intensiva o desproporcionada, configurando escenarios de control excesivo, tratamiento indebido de datos sensibles y debilitamiento de garantías constitucionales, especialmente cuando no existen criterios claros de necesidad, proporcionalidad y finalidad.

Por tanto, surge la necesidad de analizar si el uso de estas tecnologías en el sector público ecuatoriano se ajusta a los estándares constitucionales y de derechos humanos, o si, por el contrario, evidencia vacíos normativos y prácticas que podrían vulnerar derechos fundamentales.

1.4 Formulación del Problema

¿De qué manera el uso del control biométrico en el empleo público ecuatoriano, ejercido por el poder administrativo del Estado como mecanismo de vigilancia institucional, vulnera los derechos humanos de los servidores públicos ante la ausencia de una regulación jurídica específica que garantice la protección, el tratamiento adecuado y la eliminación definitiva de sus datos biométricos?

1.5 Hipótesis

El uso de tecnologías de control biométrico en el empleo público ecuatoriano llevadas a cabo por el poder administrativo del Estado como medio de vigilancia institucional, infringe los derechos humanos de los servidores públicos a partir del hecho de que la Ley Orgánica de Protección de Datos Personales del Ecuador, aplicable desde el año 2021, no establece determinadas disposiciones en lo referente al tratamiento, conservación y eliminación de datos biométricos en el marco del empleo público, lo que da lugar a un vacío normativo que no permite identificar con determinación a qué institución le corresponde eliminar dichos datos una vez extinguida la relación laboral, lo que lleva a que la vigilancia institucional operada a través del uso de la potestad administrativa del Estado sea considerada como una práctica desproporcionada que infringe los derechos a la privacidad, a la intimidad y a la autodeterminación informativa, derechos que están reconocidos por la Constitución de la República del Ecuador.

1.6 Variables

1.6.1 Variable Independiente - Tecnologías de control biométrico en el empleo público ecuatoriano

1.6.2 Variable Dependiente - Vulneración del derecho a la privacidad, intimidad, autodeterminación informativa y protección de datos personales de los servidores públicos

1.7 Objetivos

1.7.1 Objetivo General

Analizar el uso del control biométrico en el empleo público ecuatoriano y su compatibilidad con el ejercicio del poder administrativo del Estado, la vigilancia institucional y los derechos humanos de los servidores públicos, ante la ausencia de una regulación jurídica específica que garantice el tratamiento, retención y eliminación definitiva de sus datos biométricos.

1.7.2 Objetivos Específicos

1. Describir el marco normativo ecuatoriano aplicable al uso del control biométrico en el empleo público, considerando la Constitución de la República, la Ley Orgánica de Protección de Datos Personales, la Ley Orgánica del Servicio Público
2. Determinar el alcance del poder administrativo en materia de control y vigilancia laboral, identificando sus límites constitucionales frente a los derechos fundamentales de los servidores públicos al amparo de los principios de legalidad y proporcionalidad.
3. Identificar los riesgos jurídicos asociados al tratamiento de datos biométricos, considerando su naturaleza de datos sensibles y su potencial afectación a los derechos a la privacidad, intimidad y autodeterminación informativa.
4. Examinar el derecho comparado latinoamericano en materia de control biométrico en el empleo público, con el fin de extraer lineamientos regulatorios aplicables al contexto jurídico ecuatoriano.

1.8 Justificación

La justificación del presente trabajo de investigación se basa en que el Estado ecuatoriano está utilizando tecnologías biométricas de control, en el contexto del empleo público, como un mecanismo ordinario de control institucional del personal que realiza funciones en este sentido, sin que exista hasta la actualidad una regulación jurídica que determine con claridad el tratamiento, la custodia, y la eliminación de los datos biométricos de las y los servidores públicos una vez extinguida la relación de trabajo.

Efectivamente, la Ley Orgánica de Protección de Datos Personales, vigente desde el año 2021, establece principios generales sobre la protección de datos, pero no hay normas específicas aplicables al empleo público, ni tampoco se establece qué institución es la encargada de garantizar que se produzca la supresión de estos datos, lo que genera un vacío normativo que pone a las y los servidores públicos en una situación de desprotección real de sus derechos; el derecho a la privacidad, el derecho a la intimidad, el derecho a la autodeterminación informativa, derechos que están reconocidos en la Constitución de la República del Ecuador.

La importancia jurídica de esta investigación se entiende a partir de que los datos biométricos son información sensible, puesto que constituyen información sensible con calidad permanente e irrepetible, y la práctica de recogida del poder administrativo del

Estado se ha institucionalizado, así abarcando a todas las funciones del Estado ecuatoriano como la Función Ejecutiva, la Función Legislativa, la Función Judicial, y los organismos de control, sin que ninguno de, los cuales no tiene claro, obligatoria, ni armoniosamente, de su destino una vez una vez que el servidor público sale de la institución.

La gravedad de la situación se agrava, en razón que los datos biométricos, a diferencia de la información personal, en específico la incapacidad de modificación o sustitución por parte del titular: es decir, su retención indefinida o su uso administrativamente equivocado provocan un riesgo permanentemente irreversible para los derechos fundamentales del ex servidor público, quien queda abandonado de toda capacidad de control respecto de su propia información sensible frente a la institucionalidad estatal.

La investigación que se presenta a continuación cobra especial relevancia en el contexto actual, en el que acentuados avances acelerados de las tecnologías de vigilancia institucional nos colocan ante nuevos desafíos para el derecho administrativo y los derechos humanos, exigiendo que la legislación ecuatoriana evolucione de manera clandestina para adaptarse a la realidad tecnológica y asegurarse de que el ejercicio de la potestad administrativa del Estado no se convierta en un abuso que perturbe a quienes han servido a las instituciones públicas, sino que se mantenga dentro del marco que establece el Estado constitucional de derechos y justicia que encontramos consagrado en la Constitución de la República del Ecuador.

Por todo lo anteriormente expuesto, la investigación que planteamos persigue precisamente esa meta de contribuir al desarrollo normativo ecuatoriano mediante la identificación de los vacíos existentes y la propuesta de mecanismos de tutela efectiva de derechos humanos, que brinden real protección de los derechos humanos de las personas o servidores públicos ante el uso del control biométrico.

CAP II MARCO TEÓRICO

UNIDAD I Regulación del uso y control biométrico en el empleo público

Triada normativa, Constitución LOSEP Código Administrativo

Cuando una institución pública ecuatoriana instala un reloj biométrico para el registro de entrada y salida de sus servidores lo que a primera vista se perfila como una medida estrictamente administrativa, deja en evidencia la incompatibilidad de tres cuerpos normativos que obedecen a lógicas distintas.

El choque de estos cuerpos normativos refleja un problema jurídico de fondo que el Estado ecuatoriano todavía no ha resuelto, la Constitución de la República protege los datos biométricos lo que forma parte del derecho a la intimidad y a la autodeterminación informativa, la Ley Orgánica de Protección de Datos Personales califica los datos biométricos como datos sensibles y prohíbe su tratamiento salvo por excepción prevista en la ley, mientras que la Ley Orgánica del Servicio Público establece la obligación a los servidores de cumplir con su jornada, es cierto, pero nada dice sobre cómo han de cumplir su jornada, dicha combinación da como resultado un sistema de garantías en permanente tensión entre la eficiencia administrativa y la protección de derechos fundamentales sin saber encontrar un punto de equilibrio legalmente definido.

Aquí el principal punto de partida es la Constitución de la Republica esta norma delimita aquellos puntos que ninguna práctica institucional quebranta aun cuando esta práctica esté avalada por determinadas leyes secundarias. En el ámbito de los datos de carácter personal, la Constitución ecuatoriana reconoce en su artículo 66, numeral 19, que toda persona tiene derecho a la protección de los datos personales, incluyendo el acceso y el control de la información y los datos de tal carácter, así como su correspondiente protección, y que la recolección, archivo, tratamiento , distribución o difusión de los datos de carácter personal requerirán la autorización de la persona cuyo dato es objeto de tal tratamiento o el de la ley.

Dicho artículo constituye el punto de partida de toda la discusión sobre el control biométrico en la función pública, además establece como única vía para que cualquier tratamiento de datos de carácter personal sea lícito sólo dos formas: la autorización libre y expresa del titular, o bien una ley lo disponga con la suficiente concreción como para que la recolección, archivo, tratamiento, distribución la difusión de datos personales sean ejercidas como forma de autorización de ley, cualquier tratamiento de datos personales que no forme parte de ninguna de las formas válidas de autorización mencionadas será

inconstitucional desde el origen, los cuáles fueron motivos para adoptar la práctica de control biométrico.

Además, el artículo 92 de la Constitución establece la acción de hábeas data como la garantía constitucional exacta para garantizar la efectividad del derecho a la protección de datos que permite que toda persona pueda conocer qué datos suyos se encuentran en posesión de otros, quién los tiene, para qué los tiene, cuánto tiempo los conservará y con quién los compartió. Para el servidor público que ha entregado sus datos biométricos a una institución este mecanismo de hábeas data es el único instrumento constitucional directo que tiene para exigir información y control sobre su propia identidad biométrica almacenada en sistemas institucionales.

Lo que hace especialmente importante el marco constitucional que sustenta este debate es su carácter de norma aplicable directamente, en Ecuador los derechos constitucionales no requieren de ley secundaria para ser exigibles ya que, estos rigen de manera directa y obligan a todos los poderes del Estado a cumplirse incluso para las instituciones públicas en su rol de empleadores.

No obstante, es imprescindible manifestar que La Ley Orgánica de Protección de Datos Personales hace efectivo el diseño constitucional a través de reglas jurídicas y técnicas concretas. Su finalidad principal radica en garantizar el ejercicio del derecho a la protección de datos de carácter personal, determinando límites y obligaciones para quienes tratan datos junto a mecanismos jurídicos de tutela para los titulares.

Esta ley no es susceptible de operativizares como normativa legal aislada, sino que conforma parte de un propio sistema regulador definido por lo legal: normas constitucionales, penales y sectoriales, incluyendo desde 2023 con un Reglamento General, y desde 2024 y 2025 con normativa técnica y resoluciones de la Superintendencia de Protección de Datos Personales mediante los cuales se operativizan los registros, transferencias y sanciones.

Una de las aportaciones más relevantes para la discusión biométrica es la definición y clasificación del dato biométrico la LOPDP lo menciona como datos personales únicos, que pertenece a las características físicas o fisiológicas, y como conductas relativas a una persona física que permite o verifica la identificación de manera única de tal persona, considerando dentro de esto también las imágenes faciales o los datos dactiloscópicos, a la vez la norma clasifica los datos biométricos como datos de categoría especial o datos sensibles, lo que hace desplegar un régimen jurídico cualitativamente distinto respecto de aquellos que corresponden a los datos personales ordinarios.

Los principios que la LOPDP determina respecto del tratamiento de datos se consideran el segundo gran filtro que debe afrontar el control biométrico el principio de finalidad exige que los datos deben recolectarse para finalidades determinadas, explícitas y legítimas y que no deben usarse para fines distintos de las finalidades que originaron la recolección. En el momento en que el control biométrico laboral recolecta las huellas dactilares para el registro de la asistencia no pueden usarse posteriormente para otra finalidad distinta a la de controlar la asistencia, como por ejemplo aquella derivada de la identificación en una investigación interna de la empresa, control de movimientos y/o cruce con otras bases de datos.

El principio de pertinencia y minimización indica que los datos deben ajustarse a lo estrictamente necesario para la adecuación a la finalidad, la Superintendencia de Protección de Datos Personales aplicó este principio al control biométrico en el 2025 señalando que el control biométrico para registrar la asistencia no lo cumple, porque la existencia de métodos alternativos tarjetas magnéticas, registro manual, verificación de la dirección IP permiten alcanzar la misma finalidad sin la recogida de datos de categorías especiales sería suficiente.

El principio de proporcionalidad indica que el tratamiento responde a un principio de adecuación, necesidad, oportunidad, relevancia con relación a las finalidades con las que los datos han sido recolectados, el tratamiento de los datos biométricos, que además tienen la consideración de datos de categoría especial, se presenta con mayor rigor, en la LOPDP se establece que el tratamiento será proporcional no solamente con la finalidad aplicada, sino además con la misma naturaleza de las categorías especiales de datos, lo que implica un análisis de costo-beneficio donde el "peso" de los derechos restringidos debe ser inferior al beneficio obtenido.

El tratamiento de los datos biométricos debe ser proporcional, no sólo con la finalidad aplicada sino también con la misma naturaleza de las categorías especiales de datos, es importante destacar también el principio de seguridad, por su parte, este obliga a que existan medidas técnicas y organizativas adecuadas al nivel de riesgo que conlleva el tratamiento, en el caso de los datos biométricos éste es intrínsecamente elevado, lo que conlleva a la existencia de infraestructuras tecnológicas actualizadas, protocolos de acceso restringido, planes de respuesta ante este problema de seguridad y evaluaciones de impacto previas.

Este principio es el que en mayor medida entra en conflicto con la realidad de muchas de las instituciones públicas ecuatorianas en las que los sistemas tecnológicos presentan

un alto grado de obsolescencia y donde existen pocos recursos para garantizar la custodia adecuada de unos datos tan sensibles.

La Ley Orgánica del Servicio Público, en su artículo 22, literal c, prohíbe a todo servidor público el incumplimiento con dicha jornada de trabajo legalmente establecida. El artículo 25 parte del concepto de jornada ordinaria, que es una jornada de ocho horas, continuadas de lunes a viernes, con cuarenta horas semanales. El Reglamento General determina los procedimientos de control de dicha jornada y establece que las Unidades de Administración del Talento Humano son, además, las responsables del control del cumplimiento de aquella.

Hasta ahí llega la LOSEP en materia de control de asistencia, en ninguno de sus artículos remite a sistemas biométricos, a las huellas dactilares, al reconocimiento facial ni a ningún mecanismo tecnológico especifico de control , la norma sí que establece el deber de cumplir la jornada, pero el silencio normativo es absoluto sobre el cómo de verificarla. Este silencio normativo es la raíz del problema: a falta de una habilitación legal expresa que permita el uso de biometría, las instituciones públicas ecuatorianas la han ido incorporando de forma voluntaria, sin que venga contemplado en la LOSEP ningún mecanismo que lo permita y tampoco una norma de la propia ley que lo impida.

La consecuencia jurídica derivada de ese silencio es reveladora, para que tuviese lugar el tratamiento de datos biométricos de forma legítima por mandato legal, y cumpliendo con la exigencia del artículo 66, inciso 19 de la Constitución, debería establecer la LOSEP de forma explícita que la única manera que tienen los servidores para dejar constancia de su asistencia es mediante sus biometrías, y esa regla no existe.

Desde este punto el control biométrico con la relación laboral en el ámbito del empleo público ecuatoriano no satisface la exigencia del mandato legal previsto en la Constitución no puede sostenerse sólo en la voluntad del servidor, pues esa voluntad sería libre en un vínculo en el que el poder este desequilibrado.

Otro aspecto que también puede ser relevante de la LOSEP es el debate sobre el deber del servidor de custodiar y cuidar la documentación e información que por razón de su empleo le corresponde y de impedir o evitar su uso indebido. Aunque está enunciado respecto del servidor y no de la institución, establece un principio del cuidado de la información que debería trasladarse a la forma en que la propia institución debe manejar los datos de su servidor.

Uso indebido de datos biométricos y sistemas de reconocimiento facial

Diversas instituciones públicas y privadas en el Ecuador han implementado sistemas biométricos de control laboral mediante huella dactilar y reconocimiento facial para control de asistencia y acceso institucional; sin embargo, se han presentado cuestionamientos relacionados con tratamiento desproporcionado de datos biométricos, ausencia de consentimiento plenamente libre y falta de información adecuada respecto del uso y almacenamiento de datos sensibles (Velasco, 2022).

Dentro del empleo público, los servidores han manifestado preocupación respecto del almacenamiento de huellas dactilares y datos faciales sin contar con suficiente claridad sobre la finalidad del tratamiento, tiempo de conservación, medidas de seguridad implementadas, posibles transferencias de información y riesgos de filtración de datos biométricos.

Este tipo de situaciones genera problemáticas jurídicas relacionadas con el derecho a la autodeterminación informativa, privacidad y protección reforzada de datos sensibles, La Ley Orgánica de Protección de Datos Personales reconoce expresamente que los datos biométricos constituyen datos sensibles que requieren niveles especiales de protección debido a que permiten identificar de manera única e irreversible a una persona (Ley Orgánica de Protección de Datos Personales, 2021).

Estos casos evidencian la necesidad de desarrollar regulación específica sobre tecnologías biométricas y vigilancia institucional dentro del Ecuador, especialmente en ámbitos relacionados con empleo público, control administrativo y utilización de sistemas automatizados de identificación personal.

Unidad II Conflicto Real Entre Normativas Ecuatorianas

Legalización de la protección de datos personales en el estado ecuatoriano

En el Ecuador, la evolución histórica y legalización de este derecho ha representado un importante proceso de transformación jurídica orientado a fortalecer la protección de la privacidad, intimidad, dignidad humana y autodeterminación informativa frente a los riesgos derivados del uso indebido de datos personales.

El origen doctrinario de la protección de datos personales se encuentra estrechamente vinculado al desarrollo histórico del derecho a la privacidad; durante siglos, la protección jurídica de la vida privada estuvo relacionada principalmente con la inviolabilidad del domicilio, la correspondencia y la esfera íntima de las personas; el crecimiento de las tecnologías de comunicación y almacenamiento de información durante el siglo XIX

provocó la necesidad de ampliar el alcance de estas garantías frente a nuevas formas de intromisión en la vida privada.

Uno de los antecedentes más importantes corresponde al trabajo desarrollado por Warren y Brandeis, quienes plantearon por primera vez el derecho a la privacidad como "el derecho a ser dejado solo", estableciendo las bases doctrinarias modernas para la protección jurídica frente a injerencias externas en la vida privada. Esta concepción permitió posteriormente el desarrollo de nuevas categorías jurídicas relacionadas con protección de información personal.

Durante el siglo XX, el crecimiento de sistemas informáticos y bases de datos automatizadas generó profundas transformaciones dentro de la protección jurídica de la privacidad; ya que el desarrollo tecnológico permitió recopilar, almacenar y procesar enormes cantidades de información relacionada con las personas, provocando preocupaciones respecto de vigilancia estatal, control institucional y utilización indebida de datos personales.

Frente a esta realidad surgió el concepto de autodeterminación informativa, entendido como el derecho de toda persona a controlar el tratamiento de su información personal. A nivel internacional, diversos instrumentos de derechos humanos comenzaron a reconocer garantías relacionadas con privacidad e intimidad; así: la Declaración Universal de Derechos Humanos de 1948 estableció en su artículo 12 que ninguna persona puede ser objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia. Posteriormente, la Convención Americana sobre Derechos Humanos también reconoció protección respecto de la vida privada y dignidad humana.

El desarrollo jurídico de la protección de datos personales alcanzó niveles particularmente avanzados durante las últimas décadas del siglo XX; diversos países europeos comenzaron a promulgar leyes especializadas destinadas a regular el tratamiento automatizado de datos personales, estableciendo principios jurídicos relacionados con consentimiento, finalidad y seguridad informática. Posteriormente, el Reglamento General de Protección de Datos de la Unión Europea consolidó uno de los sistemas normativos más importantes a nivel mundial respecto de protección de datos personales.

En América Latina, el reconocimiento jurídico de este derecho se desarrolló progresivamente mediante reformas constitucionales y promulgación de leyes especializadas orientadas a proteger privacidad y autodeterminación informativa frente al

crecimiento tecnológico. Ecuador formó parte de este proceso regional mediante la incorporación constitucional del derecho a la protección de datos personales.

Dentro del Ecuador, uno de los hitos más importantes en la evolución jurídica de este derecho ocurrió con la promulgación de la Constitución de la República del Ecuador del año 2008 que reconoció expresamente en el artículo 66 el derecho a la protección de datos personales, incluyendo acceso, rectificación, eliminación y decisión respecto de información relacionada con las personas (Asamblea Constituyente, 2008).

Este reconocimiento constitucional convirtió a la protección de datos personales en una garantía fundamental dentro del ordenamiento jurídico ecuatoriano; también fortaleció derechos relacionados con privacidad, intimidad, honor y dignidad humana, estableciendo límites frente al ejercicio del poder estatal y frente al tratamiento indebido de información personal.

No obstante, pese al reconocimiento constitucional del derecho a la protección de datos personales, durante varios años el Ecuador careció de una normativa especializada destinada a regular integralmente el tratamiento de información personal por parte de instituciones públicas y privadas; situación que, generó vacíos jurídicos importantes frente al crecimiento de tecnologías digitales, redes sociales, plataformas electrónicas y sistemas biométricos utilizados para recopilación masiva de información.

El crecimiento tecnológico y la digitalización progresiva de servicios públicos y privados incrementaron significativamente los riesgos relacionados con filtraciones informáticas, robo de identidad, vigilancia tecnológica y utilización indebida de datos personales sensibles. Dentro de este contexto, surgió la necesidad urgente de desarrollar una legislación especializada capaz de regular principios, obligaciones y mecanismos de protección aplicables al tratamiento de datos personales.

Como respuesta a esta necesidad jurídica y tecnológica, en el año 2021 se promulgó la Ley Orgánica de Protección de Datos Personales, constituyendo el principal instrumento jurídico ecuatoriano destinado a regular el tratamiento de información personal; esta normativa representó un avance fundamental dentro del fortalecimiento del estado constitucional de derechos y justicia, debido a que estableció reglas claras aplicables tanto a entidades públicas como privadas.

La Ley Orgánica de Protección de Datos Personales reconoce principios fundamentales relacionados con; licitud, transparencia, finalidad, proporcionalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva; lo que buscan

garantizar que el tratamiento de información personal se realice de manera legítima y respetuosa de los derechos fundamentales de las personas.

La ley reconoce diversos derechos para los titulares de datos personales, entre ellos: acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión del tratamiento de datos personales. Estos derechos fortalecen la capacidad de control de los individuos respecto del uso y circulación de su información personal.

Uno de los aspectos más importantes de la legislación ecuatoriana corresponde a la protección reforzada de los datos personales sensibles, especialmente aquellos relacionados con salud, orientación sexual, ideología, origen étnico y datos biométricos. La utilización de esta información exige mayores niveles de protección jurídica debido a los riesgos de discriminación y afectación a la dignidad humana.

La legalización de la protección de datos personales también ha generado importantes obligaciones para las instituciones públicas; legalmente las entidades estatales poseen responsabilidad especial respecto del tratamiento de información personal debido a que administran enormes bases de datos relacionadas con ciudadanos, servidores públicos y usuarios de servicios estatales.

La Corte Constitucional ha señalado que la protección de datos personales constituye una manifestación directa de los derechos a la privacidad, intimidad y dignidad humana, razón por la cual toda actuación estatal relacionada con tratamiento de información debe desarrollarse bajo estricta observancia de principios constitucionales (Corte Constitucional del Ecuador, 2021).

Actualmente, la protección de datos personales en el estado ecuatoriano enfrenta importantes desafíos relacionados con implementación efectiva de la normativa, fortalecimiento institucional y adaptación frente al crecimiento de tecnologías emergentes como inteligencia artificial, reconocimiento facial y vigilancia biométrica. Asimismo, persisten limitaciones relacionadas con cultura de protección de datos, capacitación institucional y mecanismos técnicos de seguridad informática.

La legalización a través de una norma específica de la Protección de Datos es un proceso jurídico orientado a fortalecer garantías fundamentales relacionadas con privacidad, autodeterminación informativa y dignidad humana frente a los desafíos derivados de las sociedades digitales contemporáneas.

El reconocimiento constitucional y legal de este derecho constituye un importante avance dentro del ordenamiento jurídico ecuatoriano; sin embargo, su eficacia dependerá del fortalecimiento permanente de mecanismos institucionales, tecnológicos y

normativos destinados a garantizar protección efectiva de la información personal dentro del Estado constitucional de derechos y justicia.

La falta de coordinación entre las tres normas no se desenvuelve en el orden de la teoría jurídica, sino que se concreta en el momento en que un servidor público registra su huella en el marco de su entrada laboral. Ese instante es determinante el confluye tres instancias normativas que no mantienen relación: la Constitución protege esos datos como parte de la esfera íntima del servidor; la LOPDP prohíbe su tratamiento por parte del empleador salvo excepciones que en su actividad laboral ordinaria no tienen lugar; y finalmente, la LOSEP detecta la necesidad de verificar la realización de la jornada de trabajo sin especificar cómo.

La LOPDP, al ser una ley que no encuentra un marco específico para el empleo público, no afecta en su contenido los mecanismos de administración de la LOSEP, y la LOSEP, al no referirse a la LOPDP en ninguno de sus artículos, deja en manos de las Unidades de Administración del Talento Humano el decidir cuáles son las decisiones que deben tomar sobre los métodos de control de sala de asistencia, sin verse obligadas a coordinar con las exigencias de la normativa de protección de datos. Sin embargo, la Constitución prevalece por encima de ambas, pero en la práctica cotidiana de las instituciones públicas su aplicación no siempre es verificada y exigida.

El resultado es un sistema en que la protección de los datos biométricos de los empleados públicos depende más de la opción discrecional de cada institución que de un deber legal que pueda ser claro y delimitado. Algunas instituciones han ido avanzando en la adopción de políticas internas de tratamiento de datos, fruto de los criterios de la SPDP o de la presión que ejerce la misma LOPDP.

Pero muchas otras han mantenido la utilización de los sistemas biométricos sin haber hecho una evaluación de impacto, careciendo de un fundamento de legitimación debidamente documentado y ofreciendo a sus empleados públicos alternativas efectivas en el uso de la biometría.

Descubrir que este marco normativo resulta insostenible desde el punto de vista jurídico, la implementación de la LOPDP viene acompañada, entre el año 2024 y el año 2025, de normativa técnica y de resoluciones que hacen que sus exigencias sean operativas con mayor precisión, y que la SPDP empezara a ejercer en el mes de septiembre de 2024 sus funciones plenas, que se traduce en que la concepción que tiene el Estado de la capacidad de detectar y sancionar los incumplimientos es hoy mayor que en años anteriores.

Las instituciones públicas que mantienen los sistemas biométricos sin cumplir los requisitos que establece la LOPDP están asumiendo un riesgo jurídico creciente al que la impunidad normativa de la práctica anterior no garantiza que se conserve.

La solución a esta tensión exige la intervención legislativa que conecte explícitamente LOSEP con LOPDP, que pueda explicitar los métodos de control de asistencia despreciables, que decida cuál es la autonomía de las instituciones en materia de evaluación, de alternativas al uso biométrico y los plazos de conservación de los datos.

Hasta que no haya una reforma sobre estas cuestiones el funcionamiento paralelo de las tres normas seguirá vigente; el respeto de los derechos de los servidores públicos dependerá mucho más del impulso que realice cada institución que de una efectiva garantía legal.

Poder Administrativo en el control y vigilancia laboral

Cuando el Estado ecuatoriano decide poner en marcha un sistema de control biométrico para sus servidores lo hace no sólo como regulador entendiendo así que el acto es un acto normativo o como garante de derechos humanos, sino que a la vez actúa como empleador. Esta doble condición de regulador y empleador al mismo tiempo es la que genera la mayor tensión del debate que sigue al control biométrico en el empleo público. Como regulador, el Estado tiene el deber de respetar y hacer respetar los derechos fundamentales.

Como empleador, tiene potestades directivas y de control sobre lo que realizan las personas que trabajan para él, es asi que el problema es que esas dos posiciones no son siempre compatibles, y que en el caso del control biométrico éstas chocan de forma frontal.

Para entender hasta dónde llega el límite del poder administrativo en este ámbito hay que partir de lo que es la naturaleza jurídica de la potestad de dirección que el Estado ejerce sobre sus servidores y distinguirla de la que podría ser su equivalente en un empleador privado.

El poder de dirección que tiene el empleador en el derecho del trabajo es la facultad que tiene para organizar, ordenar y controlar la forma en que el trabajador presta el servicio. Esta potestad incluye el ius variandi, esto es, la facultad que tiene el empleador de modificar aspectos de la relación laboral en los límites exigidos por la ley siempre que no haya alteración sustancial de las condiciones de trabajo. Por otra parte, el ius variandi no es un derecho sin límites: está condicionado a que se realicen las modificaciones de

forma razonable, no substancial y sin que perjudiquen de manera indebida los derechos del trabajador (Scielo, 2019).

En el empleo público también existe esta potestad de dirección, pero en una forma diferente. El Estado no puede ejercitar su poder de dirección sobre los servidores públicos como podría hacerlo un empleador privado, dado que su actuación se ve además limitada por el principio de legalidad. El artículo 226 de la Constitución de la República del Ecuador establece que las instituciones del Estado, sus organismos, dependencias, la servidora o el servidor público y las personas que actúan en virtud de una potestad estatal ejercerán únicamente las competencias y facultades que les reconozca la Constitución y la ley.

Lo cual implica que el poder de control y vigilancia del Estado sobre sus servidores públicos no deriva de la autonomía privada como sucede en el caso del empleador privado, sino, por el contrario, desde un poder legalmente expresado. Justo aquí esta variable cobra una importancia excepcional en el debate biométrico. Un empleador privado puede invocar su potestad de dirección y, dentro de los ámbitos legales, adoptar métodos de control de asistencia; el Estado por su parte, necesita que tal poder esté debidamente contemplado en una norma.

Y como se pudo comprobar en la Unidad anterior, tal norma expresa no está presente tal como quedó comprobado en la LOSEP y demás cuerpos normativos ecuatorianos en cualquier caso concreto del control biométrico de asistencia. dentro de las facultades de dirección se puede identificar una manifestación específica que tiene especial relevancia para el debate biométrico: el poder de control y vigilancia. No se refiere solo a la verificación que el trabajador se encuentre adherido al conjunto de órdenes y directrices del empleador en el marco del poder directivo, sino también en la comprobación del cumplimiento del pacto laboral celebrado entre las partes y la normativa estatal, así como la verificación de las asistencias y puntualidades (Scielo, 2019).

No obstante, doctrinalmente se entiende que el poder de vigilancia y control va más allá del poder de dirección y se considera como una simple manifestación de este último pues también tiene finalidades y límites propios. El poder de vigilancia, cuando se regula a partir de la utilización de tecnologías que recogen datos de carácter personal -y muy especialmente los datos biométricos- pasa a ser un ámbito en el que los límites constitucionales se tornan más estrictos que aquellos que hace dicho control cuando de una simple instrucción laboral se trata.

La diferencia práctica es importante: el empleador incluido el Estado tiene la posibilidad de llevar a cabo una orden a un sirviente para que registre su entrada o salida, esa es sin duda una expresión legítima del poder de dirección, pero la concreción específica de tal forma de registrarse es susceptible de límites adicionales cuando es el tratamiento de datos personales de categorías especiales y exige el respeto de los derechos fundamentales por parte del trabajador; y cuando la opción elegida por el empresario vulnera tales derechos, dicha actuación de vigilancia se convierte en un acto ilegítimo, independientemente de la legitimidad del objetivo que persigue (Juris.pe, 2026).

El principio de legalidad es el eje teórico sobre el cual gira el conjunto de acciones del estado ecuatoriano, en el artículo 226 de la Constitución ecuatoriana se establece que el ejercicio del poder público solamente resulta legítimo cuando su base descansa sobre una competencia concretamente atribuida o bien por la Constitución o bien por la ley.

El artículo 14 del Código Orgánico Administrativo (COA), publicado por vez primera en el Suplemento del Registro Oficial N.° 31 de 7 de julio de 2017, establece como principio de juridicidad aquel que garantiza precisamente que la actuación administrativa se somete a la Constitución, a los instrumentos internacionales, a la ley, a los principios, a la jurisprudencia que le sea aplicable, en suma, al propio COA, y que la potestad discrecional se utilizará conforme a Derecho constituido en la Asamblea Nacional del Ecuador.

Y aquí radica la directa consecuencia que el principio de legalidad tiene sobre el control biométrico de los funcionarios públicos/as: si no hay norma jurídica que le atribuya a las instituciones públicas la facultad de recoger datos biométricos de sus servidores/as, de cara al registro de asistencia, es evidente que tal práctica carece de fundamento en el principio de legalidad, es decir, que es jurídicamente ilegítima desde el prisma del derecho administrativo, fuese cual fuese la razón que la justifique.

La investigación que fue publicada en Revistalex en el año 2025, donde da fe de esta óptica cotidiana, en el sentido que el principio de legalidad se distorsiona cuando el sistema de responsabilidades y capacidades se lleva a cabo mediante decisiones arbitrarias o sin una base normativa que lo legitime, vulnerando así el principio que establece que el Estado solamente puede actuar dentro de lo que la ley le permite expresamente (Sánchez, 2021).

El COA añade al principio de legalidad un derecho garantista complementario que afianza la discusión biométrica el Art.18 establece el principio de interdicción de la arbitrariedad que, determina que los organismos del sector público deberán emitir sus

actos conforme a los principios de juridicidad e igualdad y que no podrán llevar a cabo interpretaciones arbitrarias y que el ejercicio de las potestades discrecionales observe los derechos individuales, el deber de motivación y la razonabilidad debida.

Este principio tiene una concreción operativa en la experiencia biométrica: cuando una administración pública decide implementar un sistema de control de asistencia basado en huella dactilar o en reconocimiento facial, sin hacer una evaluación de impacto previa, sin contrastar su compatibilidad con la LOPDP y sin ofrecer alternativas a los servidores, esta decisión se calificar como arbitraria en los términos del COA, porque carece de motivación jurídica suficiente y porque no considera los derechos individuales que la Constitución garantiza.

La motivación no es un requisito formal, es una garantía sustantiva del debido proceso administrativo reconocido en el artículo 76, número 7, literal l) de la Constitución, que exige que las resoluciones de los poderes públicos sean motivadas, esto es, que expresen las normas o principios jurídicos en que se basan, así como que expliquen la pertinencia de su aplicación a los antecedentes de hecho. Por ende, una administración pública que implementa biometría sin motivar jurídicamente la decisión que toma desarrolla una actuación contraria al COA y a la Constitución.

En el debate relacionado con el control biométrico, hay un aspecto habitual que se deja de lado al centrarse en las decisiones que llegan a tomar las instituciones públicas en virtud de su competencia discrecional, es decir, por el uso de su potestad discrecional, y las que se ven obligadas a adoptar por exigencias legales, la LOSEP contempla una obligación de los servidores con relación a la jornada de trabajo, pero también ordena a las Unidades Administrativas de Talento Humano (UATH) que controlen el cumplimiento de dicha jornada: aquí tenemos una potestad reglada, porque es una potestad que está bien definida y que está obligada por la norma. La elección del método específico para controlar el cumplimiento de dicha jornada es una potestad discrecional de la UATH, puesto que no lo exige la ley.

Cuando una institución pública se ve precisada a adoptar una determinada opción a partir del ejercicio de una competencia discrecional, el COA establece en su artículo 14 que esta debe utilizarse conforme a Derecho, es decir, que la libertad en la elección del método de control de la asistencia no es absoluta, puesto que queda condicionada por los principios constitucionales, por la Ley Orgánica de Protección de Datos Personales (LOPDP) y por los principios generales de la legislación administrativa por lo que respecta a la opción por la biometría, a pesar de ser tomada por una institución a partir

del ejercicio de la competencia discrecional, ésa ha de superar los mismos estándares de razonabilidad, proporcionalidad y respeto a los derechos fundamentales, que debe superar cualquier otro acto administrativo discrecional.

El principio de proporcionalidad es del mecanismo jurídico que permite resolver problemas que surgen entre el poder del Estado, en este caso, el poder de control y vigilancia sobre los servidores y los derechos fundamentales de las personas en el ordenamiento ecuatoriano este principio es operativo en dos niveles, diferentes, pero complementarios.

A nivel constitucional, lo que establece el artículo 3 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional cuando existen contradicción entre principios o normas y la solución utilizando las reglas de solución contra la antinomias no sea posible, se aplica el principio de proporcionalidad; lo que significa que debe comprobarse que la medida que se lleva a cabo proteja un objetivo constitucionalmente permitido, sea idónea, necesaria para protegerlo y exista un adecuado balance entre protección de los derechos fundamentales y restricción constitucional.

En el ámbito administrativo es el artículo 16 del COA quien recoge el mismo principio, pero ya orientado específicamente a la actuación de las administraciones públicas, establece que las decisiones administrativas se ajustan al fin previsto en el ordenamiento jurídico y que se adoptan en un contexto del justo equilibrio entre distintos intereses, y que, llegada la hora de realizar cualquier ejercicio del derecho de las personas, no se tiene que limitar, este ejercicio a la imposición de cargas o gravámenes no desmedidos, en relación al objetivo previsto en el ordenamiento jurídico.

Esta confluencia de ambos niveles normativos hace que el principio de proporcionalidad también sea una frontera doblemente obligatoria para las administraciones ecuatorianas que implementen sistemas biométricos que deban superarla tanto en su declaración constitucional como en la administrativa.

El principio de proporcionalidad, de alguna manera, podría considerarse como la mera puesta en aplicación de una única regla, y en efecto, se despliega en tres subprincipios que deben ser aplicados de manera subsidiaria, siendo que la vulneración de alguno de los pasos implicaría la ilegitimidad de la última medida objeto de examen.

El primero de ellos no es otro que el subprincipio de la idoneidad o adecuación, que implica que la medida puesta en marcha sea verdaderamente capaz de llevarse a cabo, esto es, de alcanzar el fin que lleva consigo.

En el control biométrico se ve obligado a dar prueba de que la huella o el reconocimiento facial constituyan un medio adecuado para verificar el cumplimiento de la jornada laboral, a lo que da respuesta que la biometría resulta eficaz a la hora de identificar a una persona en un momento determinado y registrar tal extremo la idoneidad por sí misma.

El segundo subprincipio, el de la necesidad o intervención mínima, expresa que entre las distintas medidas igualmente idóneas para alcanzar el objetivo , hay que optar por la menos restrictiva de los derechos fundamentales, planteándose serias dificultades por parte del control biométrico: es que existen técnicas alternativas en la forma de tarjetas de proximidad, registros con contraseña, verificación por dirección IP, que garantizan la verificación de la asistencia digital con igual eficacia que los anteriores m é todos pero sin la necesidad de recoger datos de categoría especial.

Precisamente en este punto acaba la Superintendencia de Protección de Datos Personales concluyendo que el control biométrico para el registro de asistencia no supera el test de necesidad, por cuanto no es la opción menos intrusiva de las disponibles.

El tercero es el subprincipio de proporcionalidad en sentido estricto, que exige que los beneficios alcanzados como resultado de la medida sean mayores que los costos en términos de derechos limitados.

En el caso biométrico, la ventaja es la comprobación necesaria de la asistencia de los servidores públicos, el costo es la recolección permanente de los datos físicos irremplazables de esas personas, con el riesgo permanente de vulneración dada la situación de la infraestructura tecnológica pública ecuatoriana.

Si una entidad pública aplica un sistema biométrico sin lograr superar la prueba de proporcionalidad, y como consecuencia de que un servidor ve sus datos biométricos comprometidos en las consecuencias de una suplantación de identidad o en la vulneración de su intimidad , el Estado podría incurrir en responsabilidad objetiva , es decir , no hace falta que se acredite la intención de causar el daño: basta con confirmar que la actuación administrativa es desproporcionada y que ha producido un perjuicio real para el servidor.

La investigación publicada en sobre responsabilidad administrativa en el servicio público apunta a que, de alguna forma, el principio de proporcionalidad quedará afectado siempre y cuando las sanciones o impuestas resulten desmesuradas con relación a la gravedad de la infracción cometida o al objetivo que perseguir.

Este mismo argumento, adaptado a la biometría, viene a indicar que una medida de control que es desproporcionada para con el objetivo de comprobar la asistencia no

solamente será jurídicamente discutible: comprometerá a la responsabilidad institucional del Estado.

El dominio de la responsabilidad en materia de control biométrico desproporcionado no se atribuye singular y exclusivamente a la propia institución entendiendo la institución como una mera entidad abstracta: ya el mismo artículo 15 del COA nos avisa de que el Estado hará efectiva la responsabilidad del servidor público por actos u omisiones dolosos o culposos. En términos más sencillos, esto quiere decir que el servidor que, actuando en nombre de la institución, toma la decisión de poner en práctica el sistema biométrico sin haber llevado a cabo aquel análisis de proporcionalidad que exige la norma, o sin tener en cuenta la base que exige la LOPDP, o sin ofrecer alternativas a los propios servidores, podría, personalmente, ser responsable de los daños que la decisión pudo provocar.

Esta dimensión de la responsabilidad en forma de responsabilidad individual es de todo punto el elemento que permite introducir un incentivo real para que los funcionarios de las Unidades de Administración del Talento Humano se ocupen de realizar el análisis jurídico previo a la toma de decisiones para implementar sistemas de control con datos de categoría especial. No es una responsabilidad teórica: las evaluaciones de impacto sobre la privacidad, las consultas a la SPDP o la documentación de las bases de legitimación son procedimiento que, además de exigir su cumplimiento explícito por parte de la LOPDP, permiten al propio funcionario mirar de protegerse mejor del hecho de incurrir en una responsabilidad personal frente a decisiones que podrían ser calificadas de culpables.

El error conceptual más difundido en la discusión sobre el control biométrico en el empleo público es el de asumir que el servidor, una vez nombrado o contratado, renuncia implícitamente a ciertos derechos fundamentales a favor de la administración. Esta idea carece de fundamento constitucional.

El artículo 11, numeral 6 de la Constitución establece que los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía, por lo que la constitucionalidad del acto de renuncia no existe, y la relación jurídica incluso la relación de empleo público no aparejada una renuncia a los derechos fundamentales.

El vínculo entre el servidor público y el Estado no es uno de igualdad, existe una asimetría de poder estructural que la Constitución reconoce y que el ordenamiento jurídico debe contrarrestar. El artículo 33 de la Constitución establece que el trabajo es un derecho y deber social, es fuente de realización personal y base de la economía y el Estado garantiza a las personas trabajadoras el respeto de su dignidad y de una vida

decorosa; remuneraciones y retribuciones justas y el ejercicio de un trabajo saludable y libremente escogido o aceptado.

UNIDAD III Riesgos jurídicos del tratamiento de datos biométricos en el empleo público

El riesgo, en el marco del derecho de la protección de datos, no es un concepto que se limita a ser una mera noción abstracta o técnica: es un verdadero concepto jurídico que determina el nivel de obligaciones que han de asumir los sujetos que tratan datos personales y el nivel de protección que el ordenamiento jurídico ha de garantizar a quienes son titulares de datos personales. Tanto el Reglamento General de Protección de Datos de la Unión Europea como la Ley Orgánica de Protección de Datos Personales del Ecuador han construido sus sistemas de protección sobre una lógica de proporcionalidad al riesgo: cuanto mayor es el riesgo que supone el tratamiento, mayores son las obligaciones del responsable y más sólidas han de ser las garantías a favor del titular. En este esquema, los datos biométricos constituyen el tipo de datos personales de mayor riesgo.

La Agencia Española de Protección de Datos (AEPD), en el marco de su consulta acerca de la adecuación y la proporcionalidad de los sistemas biométricos, incidía en las Directrices del Comité Europeo de Protección de Datos (CEPD), que estableció que los datos biométricos constituyen una categoría especial tanto en el proceso de autenticación como en el de identificación, y que la identificación biométrica , que ayuda a comparar un dato contra toda una base de datos, conlleva una potencialidad mayor de afectar a los derechos fundamentales, en especial en el ámbito de la vigilancia masiva, el control social o la seguridad (AEPD, 2024).

En el caso de Ecuador, el SPDP confirmó a los afectados el acceso a los principios de 2024 y 2025 los datos biométricos requieren un nivel más elevado de protección que los otros datos de carácter personal, precisamente porque su tratamiento desmedido contiene ámbitos sensibles de la persona las mismas que se van más allá de la simple exposición de información (Gaibor Paredes, 2025).

Las diferencias entre autenticación e identificación: dos niveles de riesgo diferenciados

Un aspecto de relevancia resaltado en el análisis del riesgo en biometría que se ha desarrollado desde la doctrina especializada se encuentra en distinguir entre dos modalidades técnicas de realizar un uso de los datos biométricos que llevar a un nivel de

riesgo jurídico muy heterogéneo. La autenticación biométrica es un proceso de verificación uno a uno; consiste en comparar los datos biométricos que tiene una persona respecto de una plantilla que ya se tiene almacenada y que vinculamos concretamente con esa persona siempre con el único fin de confirmar que es quien dice ser el riesgo, por tanto, se da en una medida relativamente acotada porque el tratamiento se restringe a una comparación singular y su fin es preciso

La identificación biométrica, en cambio, es un proceso uno a varios en la que se comparan los datos biométricos que tiene una persona concretamente contra todos los que forman parte de la base de datos con la finalidad de determinar quiénes son esas personas en un universo determinado; este proceso desde la protección de datos implica regresar al conjunto de identidades ya existentes, la cual determina la existencia de riesgos para los derechos fundamentales importantes y en especial para el correcto uso de los derechos de información en situaciones como es el caso de vigilancia masiva, control social o control de seguridad.

Esta diferencia es perfectamente adecuada para el régimen de empleo público del Ecuador ya que es un sistema biométrico de control de asistencia que emplea huellas dactilares de la persona que las registra opera principalmente como un sistema de autenticación, si bien la misma base de datos que alberga dichas huellas también se puede usar posteriormente en forma de identificación, controlando al servidor en otro tipo de situaciones o cruzando su información con otras bases de datos.

El desvío de finalidad, es un riesgo estructural en estos casos, con frecuencia, no hay consentimiento expreso por parte de los titulares de los datos, e incluso incurre a que a la persona no le llegue a constar entonces es un riesgo estructural no hipotético, el deseo de fines que se producen en el control biométrico para el empleo público.

Todas las tecnologías susceptibles de controlar el comportamiento de las personas no son ajenas al diseño en el uso, esto es, a ser utilizadas en el futuro para fines diferentes de aquellas que inicialmente motivaron su diseño.

En el empleo público ecuatoriano el riesgo de desvío de finalidad se produce al menos, tres casos concretos el primero de ellos es la utilización de las bases de datos biométricos de los servidores públicos para finalidades distintas de la de control de la asistencia, como el control de la presencia en lugares o momentos no relacionados con la jornada laboral.

El segundo de los abusos es el que se produce al cruzar dicha base de datos con otros sistemas de información del Estado: nómina de registros policiales, bases de datos de seguridad social, registros de movilidad, con el objetivo de construir perfiles de conducta

de los servidores públicos a partir de datos que han sido recopilados sin contar con habilitación legal para el uso combinado. El tercer abuso, el más grave, es el intercambio de dicha base de datos con otras entidades del Estado o con contratistas privados la base de datos descrita, todo ello sin que los servidores hayan sido informados y sin que se haya contado con el consentimiento de los mismos para dicho uso adicional. El artículo 11, numeral 1 de la LOPDP establece el principio de finalidad según el cual los datos del coche personal sí lo podrán ser recopilados para fines específicos, explícitos y legítimos y no podrán ser objeto de un tratamiento incompatible con esas finalidades.

La violación de este principio, la vulnerabilidad de ese principio mediante la finalidad no exige que haya un sujeto malicioso en el acto: estas suceden por decisiones administrativas internas adoptadas sin un análisis jurídico suficiente, por órdenes de autoridades que ignoran el marco de protección de datos o como consecuencia de pura inercia de los sistemas tecnológicos que acumulan y procesan datos sin límite y más allá de lo que necesariamente exige la finalidad original.

Cuando la intención de obtener una finalidad determinada supera a partir del uso episódico (y autorizado) de los datos, de tal manera que se empieza a construir de manera sistemática patrones de comportamiento de una persona determinada a partir de la explotación de los periódicos de acceso a sus datos personales, es el momento en el que podemos de la definición de perfilamiento. El perfilamiento biométrico específico en el contexto del empleo público es especialmente peligroso porque la precisión identificativa de los datos biométricos se une a la capacidad de los sistemas actuales digitales para cruzar datos de diferentes fuentes y llegar a construir una representación exhaustiva de la vida laboral y potencialmente no laboral del servidor público.

La captura de datos biométricos de iris o de la huella dactilar, se entremezclan con otros datos de carácter personal como el lugar , el historial de entrada a los sistemas , etc. o los patrones de comportamiento, obtendría un enorme caudal de información que permitiría a construir bases de masivos datos capaces de realizar un seguimiento a la persona en Múltiples contextos, lo cual abonarían ámbitos de control social y perfilamiento que permitirían rastrear movimientos, relaciones o hábitos, todo ello sin un consentimiento real.

La evaluación de impacto como instrumento de prevención del riesgo jurídico

En la LOPDP (Ley Orgánica de Protección de Datos Personales) encontramos que a raíz del modelo del RGPD europeo, existe la obligación de llevar a cabo una Evaluación

de Impacto relativa a la Protección de Datos (EIPD) antes de cualquier tipo de tratamiento que pueda implicar un alto riesgo para los Derechos y libertades de las personas.

En este sentido, el tratamiento de datos biométricos en el empleo público se encuadra nítidamente en esta categoría, por lo que su implementación sin una previa revisión supondría, una infracción de la LOPDP, más allá del hecho de que el sistema biométrico pueda ser legítimo o no en función de determinadas circunstancias.

Este es un ejercicio jurídico y técnico que lleva a la institución a identificar los riesgos concretos del tratamiento de datos, calificar su probabilidad e impacto y describir las medidas implementadas para mitigarlos.

En el caso del control biométrico en el empleo público ecuatoriano, ese ejercicio llevaría necesariamente a identificar los riesgos de desvío de finalidad en cuanto a la discriminación y vulneración de la inseguridad que se han analizado a lo largo de este tema, y a evaluar si esos riesgos pueden mitigarse suficientemente o si justifican descartar la implementación del sistema biométrico en favor de alternativas menos riesgosas.

La ausencia generalizada de la implementación correcta de la norma en las instituciones públicas ecuatorianas que han adoptado sistemas biométricos de control de asistencia no solo representa un incumplimiento normativo: demuestra que esas decisiones fueron tomadas sin el análisis de riesgo que la LOPDP exige, lo que las convierte en actuaciones administrativas deficientemente motivadas desde el punto de vista del derecho de protección de datos.

Una de las novedades más significativas que introdujo la LOPDP en el ordenamiento jurídico ecuatoriano fue la creación de un régimen sancionador que impone consecuencias económicas y administrativas concretas a quienes traten datos personales de manera ilegítima este régimen representa un cambio cualitativo respecto a la situación anterior, en la que la protección de datos era en gran medida una obligación sin consecuencias aplicables. Como señala la doctrina especializada ecuatoriana, la introducción de ese régimen sancionador generó gran impacto, pues no solo puso en alerta a muchas organizaciones ante el riesgo de sanciones por incumplimiento, sino que también trajo un alivio para quienes durante años reclamaban un sistema legal más sólido para la tutela del derecho a la intimidad frente a constantes violaciones de privacidad (Lexis, 2025).

Unidad IV Derecho Comparado

Cuando se analiza el control biométrico en el empleo público desde una perspectiva regional, lo primero que resalta a la vista no es la diversidad de los marcos normativos, sino la uniformidad del problema central, en Colombia, en México, en Argentina y en Brasil, estos países son quienes tienen la legislación más avanzada que la de Ecuador en esta materia han tenido ya sus vulneraciones de datos biométricos de los empleados públicos.

Eso sí, la vulneración de datos no es una justificación para no regular, sino que se convierte en una idea para regular mejor, ya que pone de manifiesto que la mera aplicación tecnológica con un ineficaz sistema de control y de seguridad convierte la información biométrica del servidor en una fuente de riesgo permanente, la pertinencia del análisis se proyecta directamente sobre Ecuador.

Si los países que tienen un desarrollo institucional en la protección de datos más avanzado que el Ecuador han hecho frente a esta incapacidad para blindar la información biométrica de los servidores públicos, el Ecuador que inaugura su SPDP en el 2024 con una infraestructura pública ya envejecida, superior a los 15 años.

Incidentes Colombianos diarios de vulneración y una resolución que cambió la mirada de la biometría laboral.

Colombia es el país latinoamericano que ha documentado con más rigor la amplitud que tiene el problema de la seguridad en el tratamiento de los datos personales, informáticos y no informáticos, incluidos los biométricos, la Superintendencia de Industria y Comercio (SIC) llegó a un promedio de 100 incidentes diarios de la vulneración de datos personales durante el año 2024: más de 36.000 incidentes al año, tan sólo en los casos que llegan al conocimiento de la autoridad (Impacto, 2025).

Detrás de esos incidentes hay personas cuyos datos han sido expuestos, procesados sin ninguna autorización o utilizados en favor de finalidades diferentes de las que dieron cuenta de su recolección, en el área concreta de los datos biométricos en el ámbito del empleo, la SIC ha sido explícita en el riesgo que significa su tratamiento e investigación sin las garantías necesarias: un escape o mala utilización de datos biométricos causan consecuencias irreversibles para la identidad y la seguridad de las personas que acuden a entregarlos.

En Colombia, en el año 2024, la industria aseguradora reportó más de 30.000 casos de fraude vinculados a suplantación de identidad, con pérdidas económicas superiores a 272 mil millones de pesos colombianos.

En agosto de 2025, la SIC colombiana emitió un pronunciamiento de proyección regional que perfilaba los límites del control biométrico en relaciones subordinadas, en dicha ocasión, la SIC ordenaba a un conjunto residencial habilitar mecanismos de ingreso ajenos al tratamiento de datos biométricos y a retirar los datos biométricos de las personas residentes que así lo habían solicitado.

La SIC establecía que no es válido condicionar una actividad al suministro de datos sensibles, de tal modo que demandar datos biométricos como única condición para el ingreso se traduce en una condición desproporcionada que vulnera derechos fundamentales como el hábeas data, el de la intimidad, el de la libre circulación y la dignidad humana si alguna persona se negaba a suministrar su información sensible, entonces debían adoptarse medidas menos intrusivas, tales como las tarjetas de proximidad, códigos de acceso o el personal de seguridad formado

Aunque este caso hace referencia a una propiedad horizontal y no a una institución pública empleadora, la doctrina que establece es completamente manera extensible al empleo público: no se puede condicionar el acceso a un espacio o servicio en relación con el registro de asistencia en cualquier institución del Estado a la única posibilidad de suministrar datos biométricos cuando existen alternativas menos invasivas que permitirían cubrir las finalidades buscadas.

La magnitud de los incidentes de vulneración de la información, Colombia ha hecho esfuerzos para alcanzar el modelo de la privacidad por en su camino hacia una manera de cumplir la privacidad, la cual previene los incidentes de vulneración de la información personal (Impacto TIC, 2025); esta figura está recogida por la LOPDP que no obstante empieza a ser efectivamente utilizada por escasos organismos públicos ecuatorianos.

La privacidad por diseño se traduce en la idea de que la privacidad no es un requerimiento que va por encima del diseño de un sistema tecnológico, sino que es un requerimiento que debe entrar a formar parte de todas las fases desde la construcción, desde las configuraciones predeterminadas, etc., incluso en todas las fases que giran en torno al mismo.

Para el caso del uso público ecuatoriano, esto significaría que ninguna institución podría hacer un uso de un sistema biométrico de control de asistencia sin haber revisado desde la construcción, es decir, habiendo revisado previamente el modo de proteger

aquellos datos que recolecta, qué pasará con los datos cuando ya no sean necesarios, quién tendrá acceso a ellos o cómo se responderá ante una vulneración de la seguridad. El caso colombiano pone de manifiesto que esta figura no es solo una doctrina puede ser incluso una obligación jurídica.

México y la filtración de datos de los empleadore públicos

En 2020, México fue testigo del episodio más penoso de filtraciones de datos de servidores públicos del que se tiene constancia en América Latina desde el 6 de mayo hasta el 30 de junio de ese año, una base de datos sobre las declaraciones patrimoniales y de conflictos de interés de los servidores públicos del Gobierno federal fue expuesta y accesible para cualquier persona en internet, sin ningún tipo de restricción de acceso.

Este hecho afectó a 830.000 servidores públicos del Gobierno federal, una cifra que la propia Secretaría de la Función Pública elevó a 1,6 millones si se cuentan distintas variantes de los nombres que aparecían en la base de datos.

Lo peor no fue la magnitud de la filtración en sí, sino la respuesta institucional a esta la Secretaría de la Función Pública no sólo minimizó la gravedad de los hechos, sino que la consideró una forma alternativa de acceso a datos, el INAI, consideró el hecho como una vulneración de seguridad constatada que afecta de manera muy significativa los derechos patrimoniales de las personas titulares y en virtud de esta encontró vulneraciones a la ley de protección de datos en una resolución que fue aprobada en noviembre del 2020 por unanimidad.

El hecho, sin embargo, permaneció impune sin que haya personas responsables determinadas o responsabilidades concretas en la secretaría causante de la filtración las únicas personas que sí han sufrido las consecuencias de estos hechos han sido las personas que se han visto personificadas en esta filtración de datos.

Por un lado, infringe derechos fundamentales de las personas que le brindaron su información a cambio de su empleo por otro lado, pone de manifiesto que la asimetría de poder que caracteriza la relación de empleo público también se expresa en el ámbito de la responsabilidad: el Estado es el que tiene los datos, el que estipula de qué manera se protegen y, en caso de negligencia, rara vez es el mismo Estado el que paga las consecuencias, las cuales, por otro lado, quedan en manos de las víctimas de manera duradera.

La filtración de las claves del gobierno de 2020 no fue un evento puntual en México. Entre 2018 y 2025, el gobierno mexicano sufrió importantes consecuencias de datos que comprometieron información muy sensible y que le afectaron en su operación. Entre los

eventos más relevantes se encuentra el ciberataque de 2024 a la Consejería Jurídica de la Presidencia del Estado, perpetrada por el grupo y desvelando 206 GB de datos; el ataque masivo perpetrado en 2022 a la Secretaría de la Defensa Nacional por parte del colectivo Guacamaya que llevó a la revelación de siete terabytes de documentos clasificados esta información era de seguridad en las dependencias de la Lotería Nacional, de la Comisión Nacional del Agua y de la plataforma Llave CDMX, en las que se mostraban incluso datos de actores políticos estas vulneraciones incluían el acceso no autorizado a datos de empleados

Lo que hace especialmente relevante el caso mexicano para Ecuador es la explicación de por qué ocurren estas vulneraciones la unidad de investigación de SILIKN determinó que la fuga de información fue causada por actividades de empleados antiguos o actuales que vendieron o compartieron credenciales con los grupos cibercriminales, así como por la introducción de ciertos tipos de malware orientados a robar información para comprometer a un amplio segmento de empleados de las dependencias

Esta situación en la que la base de datos que recopila a los empleados públicos son simultáneamente el objetivo del ataque cibercriminal y el canal directo por el cual el atacante logra acceder al sistema se convierte precisamente en el riesgo que se incrementa cuando las instituciones públicas comienzan a realizar procesos de levantamiento de datos biométricos de sus servidores sin las necesarias garantías en seguridad; los mismos datos que eran usados para identificar al servidor se convierten en la vía que hace posible suplantar la identidad del servidor dentro del sistema de la institución pública.

La nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que pasó a ser efectiva el 21 de marzo de 2025, determinó con mayor severidad la obligación de recabar de nuevo el consentimiento para el supuesto de que se fueron a tratar datos personales para finalidades distintas de las inicialmente previstas, toda vez que ya no se permitiría la posibilidad de tratar datos bajo consentimientos genéricos (México, 2025).

Esta reforma representa una respuesta a los abusos que pudieron documentarse en el tratamiento de datos de servidores públicos: el Estado mexicano reconoció que el consentimiento que se observaba para el ingreso al empleo no podía usarse indefinidamente para cualquier tratamiento posterior de los datos del servidor.

3.1.4 Brasil como víctima de su propia deficiencia de seguridad

Brasil es un caso que merece atención particular dentro del derecho comparado latinoamericano, no porque sea el peor ejemplo en materia de protección de datos, sino

precisamente porque es el más ilustrativo de una realidad que Ecuador debe comprender antes de que le ocurra lo mismo: tener una ley no es suficiente si esa ley no va acompañada de una autoridad capaz de hacerla cumplir desde el primer día.

La Ley General de Protección de Datos Personales de Brasil, conocida como LGPD, fue aprobada en agosto de 201 sin embargo, el gobierno brasileño estableció la Autoridad Nacional de Protección de Datos por decreto recién a finales de agosto de 2020, dos años después. Y aunque la norma que ordena su creación era la única parte de la LGPD que estaba en vigor desde diciembre de 2018, durante todo ese período la nueva autoridad no había emitido ningún reglamento, ya que aún estaba en proceso de ser literalmente construida desde cero. La orientación sobre cómo auditar bases de datos personales, especialmente en materia de seguridad, era simplemente inexistente. En ese contexto, el gobierno anunció la próxima creación de un nuevo sistema de identidad digital, lo que significa que mientras la institución encargada de proteger los datos de los brasileños todavía no existía de manera operativa, el Estado avanzaba en la implementación de sistemas que recolectarían aún más información personal de la ciudadanía.

Esta promulgación de la norma y la existencia real de la autoridad que debía hacerla cumplir es la primera lección que Brasil aporta al debate ecuatoriano , Ecuador aprobó su LOPDP en 2021 y la SPDP recién inició funciones plenas en 2024. Tres años de vacío operativo en los que instituciones públicas y privadas continuaron implementando sistemas biométricos sin que existiera un organismo con capacidad real para fiscalizar, auditar y sancionar esas prácticas.

Las consecuencias de ese vacío institucional se hicieron evidentes de la manera más dramática posible en enero de 2021, cuando se descubrió en Brasil la filtración de datos personales de más de 220 millones de ciudadanos y empresas, ofrecidos a la venta en la web oscura. La firma de seguridad PSafe descubrió el incidente, que reveló todo tipo de datos personales, incluyendo información vinculada al modelo de segmentación de consumidores utilizado por Serasa Experian, la filial brasileña de la multinacional Experian. Esta filtración ha sido comparada con el caso Equifax en Estados Unidos, donde fueron expuestos los datos de 145 millones de personas, aunque en el caso brasileño la magnitud fue aún mayor en términos absolutos.

Lo que hace jurídicamente extraordinario este caso es su contexto normativo: ocurrió después de que Brasil hubiera aprobado su nueva ley de protección de datos, pero antes de que esa ley tuviera una autoridad operativa capaz de sancionar a los responsables y antes de que las sanciones por incumplimiento pudieran ser aplicadas, ya que estas no

comenzaron a ser efectivas hasta agosto de 2021. Esto significa que en el momento en que se produjo la filtración más grande de la historia de América Latina, Brasil tenía una ley, pero no tenía el sistema institucional para hacerla valer. El resultado fue que la empresa responsable respondió a las autoridades afirmando que todas sus actividades cumplían con las regulaciones brasileñas de protección de datos, sin que existiera un mecanismo efectivo inmediato para controvertir esa afirmación o sancionar la conducta.

Para Ecuador, esta experiencia tiene una lectura directa y preocupante. Así como Brasil experimentó su mayor crisis de datos durante el período de transición entre la aprobación de la norma y el funcionamiento pleno de su autoridad de control, Ecuador se encuentra todavía construyendo la capacidad institucional de la SPDP, mientras que las instituciones públicas siguen recolectando datos biométricos de sus servidores en sistemas cuya seguridad nadie ha auditado de manera sistemática.

Otro aspecto central de la problemática brasileña anterior a la LGPD fue la dispersión normativa. Antes de la aprobación de esa ley, el tratamiento de datos personales en Brasil estaba regulado por más de cuarenta estatutos diferentes que gobernaban los datos personales de manera fragmentada y contradictoria. Cada sector tenía sus propias reglas, con distintos niveles de protección, distintas definiciones de dato personal y distintos mecanismos de sanción. Esta fragmentación hacía prácticamente imposible que un ciudadano común pudiera conocer sus derechos frente al tratamiento de sus datos, y que una autoridad pudiera aplicar estándares uniformes de fiscalización.

Los datos biométricos, en particular, no tenían una regulación específica dentro de ninguno de esos cuarenta estatutos. Esto significa que, durante décadas las instituciones brasileñas públicas y privadas recolectaron datos biométricos de trabajadores y ciudadanos sin que existiera ninguna norma que definiera qué eran esos datos, cómo debían protegerse, quién podía acceder a ellos ni cuánto tiempo debían conservarse. El trabajador que entregaba su huella dactilar para registrar su asistencia en una institución pública lo hacía en un vacío jurídico total: no existía ningún instrumento que le dijera qué ocurriría con ese dato al día siguiente, al año siguiente o cuando dejara de trabajar en esa institución.

Ecuador tomó un camino más directo al crear la LOPDP como norma unificada, pero la fragmentación persiste en un sentido distinto no tiene vasos comunicantes con la LOSEP, con el Código del Trabajo, ni con los reglamentos de las distintas instituciones públicas. El resultado práctico es similar al de Brasil antes de la LGPD: cada institución pública ecuatoriana toma sus decisiones sobre el tratamiento de datos biométricos de sus

servidores en función de sus propias interpretaciones, sin que exista un marco operativo uniforme que garantice estándares mínimos comunes.

Una de las deficiencias más graves que la doctrina ha identificado en el sistema jurídico brasileño anterior a la LGPD es que los datos biométricos no tenían una definición legal expresa. Aunque la práctica biométrica ya estaba extendida en el empleo público y privado, ninguna norma establecía con precisión qué era un dato biométrico, en qué se diferenciaba de otros datos personales y por qué merecía un nivel de protección superior. Esta ausencia de definición no fue un olvido inocente: tuvo consecuencias reales sobre la protección de los trabajadores.

Sin una definición legal, las instituciones que recolectaban huellas dactilares o imágenes faciales de sus empleados podían argumentar que esos datos eran simplemente datos de control de asistencia, sin ninguna diferencia jurídica respecto a un registro manual de entrada y salida. La posibilidad de usar esa información para perfilar, discriminar o vigilar a los trabajadores más allá del ámbito laboral quedaba en un limbo jurídico donde nadie era responsable de prevenir el abuso porque nadie estaba legalmente obligado a reconocer que esos datos eran especialmente sensibles.

La LGPD resolvió ese problema al incluir los datos biométricos de manera expresa en la categoría de datos sensibles, estableciendo que su tratamiento requiere bases de legitimación específicas y condiciones de seguridad reforzadas. Sin embargo, como señaló la investigación de openDemocracy en 2021, el hecho de que la ley existiera no impidió la filtración más grande de la historia brasileña, porque la ley sin la autoridad que la haga cumplir es tan ineficaz como la ausencia de ley la diferencia es solo formal: el daño a las personas es igual de real.

Adicionalmente, la LGPD no estableció desde el inicio un mecanismo específico para el tratamiento de datos biométricos en el contexto del empleo público, limitándose a clasificarlos como datos sensibles con reglas generales de tratamiento. Como consecuencia, muchas instituciones públicas brasileñas continuaron implementando sistemas biométricos de control de asistencia sin haber realizado las evaluaciones de impacto que la propia ley exigía, precisamente porque la norma no establecía de manera suficientemente clara que esa obligación era aplicable también al empleo público en el contexto del control laboral ordinario.

CAPÍTULO III: MARCO METODOLÓGICO

3 MÉTODO DE INVESTIGACIÓN

La presente investigación se lleva a cabo bajo un enfoque cualitativo que hace posible conocer a fondo la realidad social, jurídica e institucional en relación con el control biométrico en el empleo público en el Ecuador, ya que el enfoque cualitativo pone el acento en la interpretación del contexto normativo, administrativo de los derechos humanos, en función de que el objeto de estudio requiere de una crítica de significados a la vez que de estructuras jurídicas

3.1 Tipo de Investigación

Cualitativa: Se enfoca en analizar e interpretar de manera integral los mecanismos teóricos, las percepciones y las implicaciones jurídicas que rodean la adopción de tecnologías biométricas en el sector público.

Este enfoque permite examinar la naturaleza del fenómeno desde la óptica del respeto a los derechos humanos y los límites del poder administrativo, priorizando la comprensión profunda de las normas y la doctrina jurídica.

Cuantitativa: Se plantea mediante la recopilación y el análisis de datos empíricos obtenidos a través de instrumentos aplicados a un grupo específico de actores clave (como servidores públicos). Su propósito es medir, cuantificar y estructurar estadísticamente variables relacionadas con el nivel de cumplimiento normativo, la frecuencia de uso de estos sistemas y el impacto real de la biometría en la protección de datos personales.

Exploratorio: Se basó en la búsqueda, revisión e indagación sistemática dentro de diversos mecanismos teóricos, y antecedentes normativos internacionales y nacionales. Este nivel es fundamental para aproximarse a un fenómeno dinámico y en constante evolución en el ordenamiento jurídico ecuatoriano, sentando las bases conceptuales para identificar vacíos legales sobre la transformación digital del Estado.

3.2 Técnicas e instrumentos de investigación

La técnica principal de recolección de información utilizada en esta investigación fue la revisión documental y el análisis de la misma,

De manera complementaria, se incluyó la recolección de información, como entrevistas interpretativas y las encuestas, la cual permitió realizar una evaluación del

alcance, de la normativa jurídica ecuatoriana sobre la implementación de sistemas biométricos en la administración pública.

3.3 Criterio de Inclusión y Criterio De Exclusión

Como criterios de inclusión se recogen fuentes de información de carácter jurídico, académico o doctrinal que tengan directa relación con el uso del control biométrico en la administración pública, el derecho administrativo, el derecho constitucional, y la protección de datos personales. Se han tenido en cuenta normas vigentes en el ordenamiento jurídico ecuatoriano, especialmente las reglas que tienen que ver con el empleo público, la transformación digital del Estado y las garantías de derechos fundamentales.

Del mismo modo, **como criterios de exclusión** se contemplaron aquellos estudios que se encuentran desactualizados, además de ello aquellos que no responden al marco normativo de la actualidad o que no responden a la época actual de la transformación digital del Estado ecuatoriano, puesto que esto podría afectar la validez del análisis jurídico.

3.4 Unidades de Análisis (Población y Muestra)

Población

La población de estudio de la presente investigación estuvo conformada por 200 servidores públicos quienes ocupan el principal objeto de análisis

Muestra

Para la presente investigación se tomó una muestra significativa que permitiera conocer la realidad que se vive en la ciudad de Guaranda por tanto se por lo que la muestra estuvo conformada por 3 expertos en la materia con el objeto de profundizar un análisis técnico jurídico del ejercicio del poder administrativo en la utilización de las tecnologías biométricas.

3.5 Localización geográfica de estudio

El lugar donde se desarrollo fue en la ciudad de Guaranda, provincia Bolívar

1. Capítulo IV: Resultados y Discusión

4. Resultados

En este ámbito territorial, la recogida de la información se llevó a cabo a través de entrevistas semiestructuradas, realizadas a personas que actuaban como actores clave vinculados a la gestión institucional y al uso de tecnologías en el ámbito del sector público.

Entre las personas entrevistadas, encontramos al Directora de Talento Humano, quien es la persona responsable de la administración de personal y del control de la asistencia por medio de los sistemas biométricos; al Director de la Gestión de Tecnologías de la Información, al frente de la implementación y administración de los sistemas tecnológicos institucionales; una abogada del ámbito de la protección de datos personales, quien realizó un análisis jurídico especializado acerca de la garantía de los derechos fundamentales frente al tratamiento de datos biométricos.

Resultados de las Entrevistas a los diferentes Profesionales

1.- Desde su perspectiva profesional ¿cuál es su criterio respecto al marco constitucional, legal y de protección de datos personales que regula el uso del control biométrico en el empleo público ecuatoriano, y usted como considera que este se aplica en la práctica dentro de las instituciones públicas en relación con la vigilancia institucional, el poder administrativo y la garantía de derechos humanos de los servidores públicos?

Tabla 1

Ing. Galo Sanany	Considero que su aplicación no puede entenderse como un mecanismo de control absoluto, sino como una herramienta administrativa que debe respetar los principios de legalidad, necesidad, proporcionalidad y finalidad, evitando cualquier forma de vigilancia excesiva dentro del entorno laboral público. Asimismo, su tratamiento debe garantizar condiciones adecuadas de seguridad de la información, confidencialidad y uso exclusivo para fines institucionales previamente determinados por la normativa vigente Es por ello que el uso de tecnologías biométricas dentro del empleo público deben ajustarse principalmente a la Constitución de la República del Ecuador, especialmente respecto de derechos relacionados con privacidad, intimidad y protección de datos personales; además, las instituciones públicas debemos observar lo establecido en la Ley Orgánica del Servicio Público y en la Ley

	Orgánica de Protección de Datos Personales, debido a que los datos biométricos constituyen información sensible que requiere protección especial..
Lic Hipatia Ballesteros	Es fundamental mencionar que los sistemas que van a ser implementados cuenten con medidas técnicas adecuadas como cifrado de información, control de accesos y trazabilidad de los registros, a fin de garantizar la integridad de los datos y evitar su uso indebido o filtraciones. El tratamiento de datos biométricos debe cumplir los principios de seguridad, confidencialidad y proporcionalidad establecidos en la Ley Orgánica de Protección de Datos Personales, el Código Orgánico Administrativo y las políticas institucionales internas regulan el manejo de sistemas tecnológicos utilizados para control laboral y autenticación de usuarios. Asimismo, se debe tomar en cuenta la gestión de estas tecnologías debe orientarse únicamente a fines administrativos legítimos, asegurando que su utilización no exceda los límites establecidos por la normativa vigente ni afecte los derechos fundamentales de los servidores públicos.
Abg. Carola López	La legislación ecuatoriana reconoce explícitamente la protección, constitucionalmente garantizada, de los datos personales que viene dada, entre otras, por la competencia que confiere el artículo 66 numeral 19 de la Constitución de la República del Ecuador. Vale la pena agregar a este asunto la Ley Orgánica de Protección de Datos Personales, que estipula las reglas adecuadas para el tratamiento de la información sensible, dentro de la cual se encuentran también los datos biométricos como los que tienen que ver con las huellas dactilares, pero también con el reconocimiento facial. Desde mi punto de vista, su uso catalogado bajo la actual normativa laboral pública debería atenerse con suma rigurosidad a todos los principios de legalidad, finalidad, proporcionalidad y minimización de datos. Y es que no se trata de introducir nuevas tecnologías en el empleo público por modernizarlas, sino que debe hacerse con una justificación materialmente real y necesaria para la institución, e, incluso, de acuerdo a ello, con el

	avituallamiento de la información que debe ser utilizada solo para los fines institucionales permitidos por la ley.

Investigador: *Fernanda Mishel Guacho Auquilla*

Análisis

A partir de la información obtenida en las entrevistas y de la normativa revisada, queda claro que la utilización de las tecnologías de control biométrico en la Administración Pública ecuatoriana transita en una tensión clara entre la modernización administrativa del Estado y la práctica real del deber de proteger los derechos fundamentales de los servidores públicos.

Por una parte, la visión que nos ofrecen las áreas jurídicas y administrativas.es que la adopción de los sistemas biométricos está vinculada a necesidades institucionales legítimas, como la verificación de asistencia, la verificación de la identidad y la mejora los procesos de administración del talento humano.

2.- ¿Hasta qué punto la administración pública puede ejercer el control institucional sobre los servidores públicos mediante el uso de tecnologías biométricas sin vulnerar los derechos constitucionales relacionados con la privacidad y la protección de datos personales?

Tabla 2

Ing. Galo Sanany	Si bien es cierto, la administración pública cuenta con facultades para controlar la asistencia y el cumplimiento de las obligaciones laborales de los servidores públicos; considero que dicho control debe mantenerse dentro de parámetros razonables y debidamente justificados, respetando en todo momento los derechos fundamentales de los trabajadores y evitando la implementación de mecanismos de vigilancia excesiva o desproporcionada. En este sentido, el uso de tecnologías biométricas debe orientarse exclusivamente a fines administrativos legítimos, garantizando la protección de la privacidad, la intimidad y los datos personales de los servidores públicos, de manera que el ejercicio del poder institucional no implique una afectación a sus derechos constitucionales.
Lic Hipatia Ballesteros	Las tecnologías biométricas pueden ser herramientas muy útiles para fortalecer la seguridad institucional y mejorar la eficiencia en los

	procesos administrativos; sin embargo, su uso debe manejarse con mucha responsabilidad y estar claramente regulado. Desde mi perspectiva, es importante que estas tecnologías se apliquen únicamente para fines específicos y previamente establecidos por las instituciones, de modo que no se desvirtúe su propósito. Asimismo, debe cuidarse que no terminen convirtiéndose en mecanismos de vigilancia constante o excesiva, ya que esto podría afectar la privacidad y los derechos fundamentales de los servidores públicos.
Abg. Carola López	Hay que mencionar que el poder administrativo permite implementar mecanismos de supervisión laboral; sin embargo, este no puede ejercerse de manera ilimitada, ya que toda medida que implique el uso de tecnologías biométricas debe someterse a un análisis riguroso de proporcionalidad y necesidad. Esto se debe a que el Estado no puede justificar afectaciones a la privacidad o a la autodeterminación informativa únicamente con argumentos de eficiencia administrativa. En este sentido, considero importante señalar que la implementación de estos sistemas debe ir acompañada de garantías claras que protejan los derechos de los servidores públicos,

Investigador: *Fernanda Mishel Guacho Auquilla*

Análisis

Las tecnologías biométricas en el empleo público ecuatoriano se han convertido en una herramienta útil para mejorar el control de asistencia, la organización institucional y la eficiencia administrativa. Su uso facilita procesos internos y aporta mayor seguridad en la gestión del personal.

Sin embargo, su aplicación también implica el tratamiento de datos personales sensibles, lo que obliga a manejarlas con responsabilidad. El principal punto de atención está en que estas tecnologías no deben afectar derechos como la privacidad y la protección de datos de los servidores públicos.

3.- ¿Qué naturaleza jurídica tienen los datos biométricos y cuáles son los principales riesgos que se generan al tratarlos dentro del sector público ecuatoriano, especialmente en el marco del control laboral y la protección de derechos fundamentales de los servidores públicos?

Tabla 3

Ing. Galo Sanany	Es importante analizar que los datos biométricos son información altamente sensible, ya que permiten identificar de forma directa a una persona. Desde la experiencia en talento humano, se puede ver que uno de los principales riesgos es la filtración de esta información, el acceso no autorizado o incluso su uso para fines distintos a los que fueron establecidos por la institución, lo que puede generar preocupación respecto a la privacidad de los servidores públicos.
Lic Hipatia Ballesteros	Es necesario tomar en cuenta que, desde el ámbito técnico, los datos biométricos requieren un nivel muy alto de protección, ya que tienen una particularidad importante: no se pueden cambiar. A diferencia de una contraseña, si esta información se vulnera, no existe forma de reemplazarla, por lo que cualquier falla en la seguridad puede tener consecuencias serias para la persona.
Abg. Carola López	Es relevante mencionar que, desde el punto de vista jurídico, los datos biométricos son considerados datos personales sensibles según la Ley Orgánica de Protección de Datos Personales. En este sentido, si no se manejan adecuadamente, pueden llegar a afectar derechos fundamentales como la privacidad, la autodeterminación informativa e incluso la dignidad de las personas, sobre todo si se utilizan sin una justificación clara o de forma excesiva.

Investigador: *Fernanda Mishel Guacho Auquilla*

Análisis

Desde la óptica administrativa y de las personas trabajadoras, en consecuencia, el riesgo por filtraciones de información, accesos no autorizados y por el uso incorrecto de los datos para otros fines que no sean los institucionales son lo que han de destacarse. Esto pone nuevamente de manifiesto que es necesario instrumentar controles internos muy claros y bastante estrictos sobre su tratamiento.

En el terreno técnico, hay además que resaltar una de sus características más importantes: la irreversibilidad de los datos biométricos, pues, a diferencia de otras formas de autenticación, no pueden ser modificados tras una situación de vulneración, aspecto que determina la importancia de disponer de sistemas de seguridad informática muy robustos y fiables.

4.- ¿En qué medida la implementación de sistemas biométricos cumple con los principios de protección de datos personales establecidos en la legislación ecuatoriana?

Tabla 4

Ing. Galo Sanany	Es importante analizar que todavía existen ciertas limitaciones en la forma en que se están implementando los sistemas biométricos en el empleo público. En la práctica, muchas instituciones los utilizan principalmente para el control de asistencia, pero no siempre se brinda información clara y suficiente a los servidores públicos sobre cómo se usan, almacenan o protegen sus datos biométricos. En este sentido, es imprescindible fortalecer la transparencia, para que las personas tengan mayor conocimiento y confianza sobre el manejo de su información.
Lic Hipatia Ballesteros	Es necesario tomar en cuenta que, desde el área tecnológica, aunque se busca cumplir con estándares de seguridad, todavía existen varios retos. Entre ellos están la actualización constante de los sistemas, la realización de auditorías periódicas y la capacitación del personal sobre protección de datos. En este punto, es imprescindible seguir fortaleciendo estos aspectos para garantizar que las plataformas biométricas funcionen de manera segura y adecuada.
Abg. Carola López	Es relevante mencionar que, desde el enfoque jurídico, en algunos casos la implementación de estos sistemas aún no cumple completamente con principios como la proporcionalidad, la minimización de datos y la transparencia. Se han identificado instituciones que recopilan información biométrica sin realizar evaluaciones previas o sin justificar del todo su necesidad. .

Investigador: *Fernanda Mishel Guacho Auquilla*

Análisis

A partir de las respuestas recabadas, puede constatarse que la implementación de las tecnologías biométricas al servicio del empleo público presenta todavía algunas barreras operativas. Si bien es cierto que son herramientas que se utilizan, en general, para el control de asistencia y para gestionar la organización interna, la mayoría de las veces no

se facilita la información necesaria a los servidores públicos en referencia a qué se hace con sus datos, lo que provoca una cierta inquietud.

Se puede evidenciar además que desde la perspectiva técnica todavía persisten obstáculos importantes, como el de mantener el sistema actualizado, realizar controles de seguridad periódicos y la formación del personal responsable, lo cual es básico a la hora de evitar fallos y proteger la información de los usuarios.

5.- ¿De qué manera la implementación de tecnologías biométricas en el empleo público ecuatoriano está generando dificultades en su aplicación práctica, especialmente en relación con la falta de información a los servidores públicos, los retos técnicos de seguridad y la posible inobservancia de principios jurídicos como la proporcionalidad, la transparencia y la necesidad en su uso?

Tabla 5

Ing. Galo Sanany	Entendiendo el ámbito de la gestión del Talento Humano, creo que una de las principales desventajas es que no se explica adecuadamente a los trabajadores en el sector público el modo en que se gestionan los datos biométricos. En la práctica es cierto que se implantan para controlar la asistencia, pero no siempre se aclara para qué acceder a la información, en qué lugar se almacenan o con qué otros fines podrían utilizarse, lo que va a hacer que lleguen a suscitar dudas o incertidumbres en el personal.
Lic. Hipatia Ballesteros	Desde la parte tecnológica, se puede extraer que uno de los problemas más importantes es la seguridad de los sistemas, porque no siempre se dispone de equipos que pueden estar completamente actualizados ni se realizando auditorías periódicas, lo que puede hacer aumentar el riesgo de fallos en la seguridad de dichos sistemas. También creo que es importante la formación constante del personal, ya que el buen uso de estas herramientas es muy importante para proteger la información y que no se generen problemas.
Abg. Carola López	Desde un punto de vista jurídico, se puede evidenciar que, en algunos casos, sí se aplican de manera parcial los principios de proporcionalidad, transparencia y necesidad en la implementación de sistemas biométricos dentro del empleo público. En ciertas instituciones, no siempre se justifica de forma suficientemente clara

	la necesidad de utilizar este tipo de tecnologías ni se realizan evaluaciones o auditorías previas y continuas una vez que el sistema entra en funcionamiento. Esto puede resultar problemático, por lo que es importante hacer énfasis en que su uso debe estar siempre debidamente regulado y controlado, garantizando que no se afecten en ningún momento los derechos de los servidores públicos.

Investigador: *Fernanda Mishel Guacho Auquilla*

Análisis:

En cuanto al nivel organizativo institucional se aprecia que hay problemas de comunicación, de dar aviso a los servidores públicos sobre el trato de datos biométricos, ya que se tiene incertidumbre sobre quién tiene acceso, cómo lo almacena o cómo lo trata. Lo que parece indicar que debe reforzarse la transparencia institucional. En segundo lugar, a nivel técnico se ven obstáculos relativos a la actualización de los sistemas, a la falta de auditorías o de formación a los equipos encargados. Esto puede repercutir tanto en la seguridad de la información, generando riesgo de fallos o bien vulneración de los datos, como para otros aspectos también sensibles.

Interpretación de los resultados que se obtuvo en las encuestas que se aplicaron a servidores públicos que utilizan el Control Biométrico en el cantón Guaranda

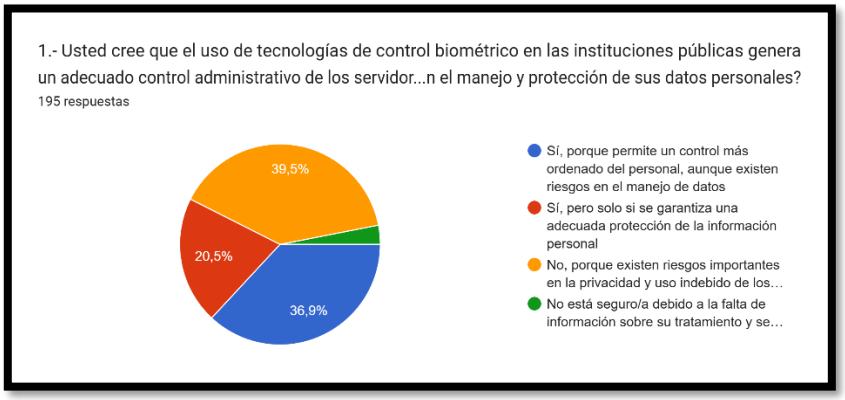
Pregunta 1

¿Usted cree que el uso de tecnologías de control biométrico en las instituciones públicas genera un adecuado control administrativo de los servidores públicos, considerando la problemática existente en el manejo y protección de sus datos personales?

Tabla No. 1

Opción	Cantidad	Frecuencia
No, porque existen riesgos importantes en la privacidad y uso indebido de los datos	82	41%
Sí, porque permite un control más ordenado del personal, aunque existen riesgos	72	36%
Sí, pero no se garantiza una adecuada protección de la información personal	40	20%
No está seguro/a debido a la falta de información sobre su tratamiento y seguridad	6	3%
TOTAL	**200**	**100%**

Gráfico No. 1



Investigador: *Fernanda Mishel Guacho Auquilla.*

Población: *Servidores públicos, Cantón Guaranda, Provincia de Bolívar.*

Análisis: De los resultados obtenidos en la encuesta aplicada a 200 servidores públicos, respecto a la relación entre el control administrativo y la salvaguarda de la información personal, se evidencia que el 41% de los participantes sostiene una postura crítica, afirmando que estas herramientas no generan un manejo institucional adecuado debido a los riesgos sustanciales en la privacidad y el uso indebido de los datos.

En contraste, un 36% considera que la medida sí permite un ordenamiento más eficaz del personal a pesar de admitir la existencia de dichos riesgos, mientras que un 20% señala que, aunque el control es adecuado, no se garantiza una verdadera protección de la información personal, quedando un 3% en la incertidumbre debido a la falta de información sobre su tratamiento y seguridad. Estos resultados consolidan el 100% de la muestra evaluada.

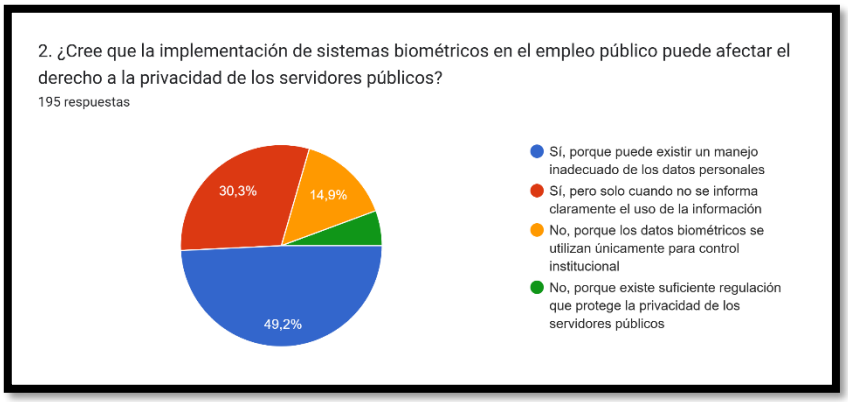
Pregunta 2

¿Cree que la implementación de sistemas biométricos en el empleo público puede afectar el derecho a la privacidad de los servidores públicos?

Tabla No.2

Opción	Cantidad	Frecuencia
Sí, porque puede existir un manejo inadecuado de los datos personales	96	48%
Sí, pero solo cuando no se informa claramente el uso de la información	64	32%
No, porque los datos biométricos se utilizan únicamente para control institucional	29	14.5%
No, porque existe suficiente regulación que protege la privacidad de los servidores	11	5.5%
TOTAL	**200**	**100%**

Gráfico No. 6



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis: Al consultar sobre la posible afectación al derecho fundamental a la privacidad, el 48% de la muestra asegura de forma directa que estos sistemas sí vulneran dicha garantía debido a la probabilidad de un manejo inadecuado de la información personal. A esta percepción se suma un 32% que sostiene que la afectación se produce específicamente cuando las instituciones no informan de manera clara el uso de la información. Por otro lado, un 14.5% descarta cualquier tipo de impacto negativo argumentando que los datos se emplean únicamente para control institucional, y finalmente, un 5.5% confía en que no existe vulneración porque hay suficiente regulación que protege la privacidad de los servidores, completando así el 100% de las respuestas.

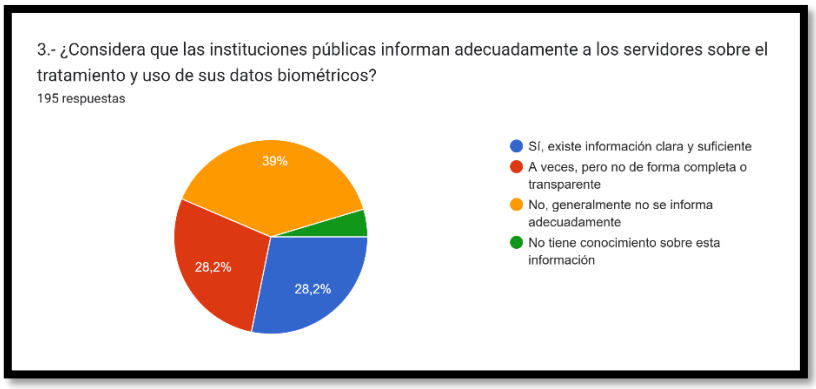
Pregunta 3

¿Considera que las instituciones públicas informan adecuadamente a los servidores sobre el tratamiento y uso de sus datos biométricos?

Tabla No.3

Opción	Cantidad	Frecuencia
No, generalmente no se informa adecuadamente	81	40.5%
Sí, existe información clara y suficiente	55	27.5%
A veces, pero no de forma completa o transparente	55	27.5%
No tiene conocimiento sobre esta información	9	4.5%
TOTAL	**200**	**100%**

Gráfico No. 3



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis:

Al evaluar el cumplimiento del deber de información por parte de las entidades estatales, el 40.5% de los participantes manifiesta de manera categórica que las instituciones generalmente no informan de forma adecuada sobre el uso y alcance de estos sistemas. Por su parte, las posturas se dividen equitativamente entre quienes afirman que sí existe información clara y suficiente (27.5%) y quienes perciben que esta se entrega solo a veces y de forma incompleta o poco transparente (27.5%). El restante 4.5% indica no tener conocimiento sobre esta información, evidenciando en conjunto (100%) un importante lazo en la comunicación interna institucional.

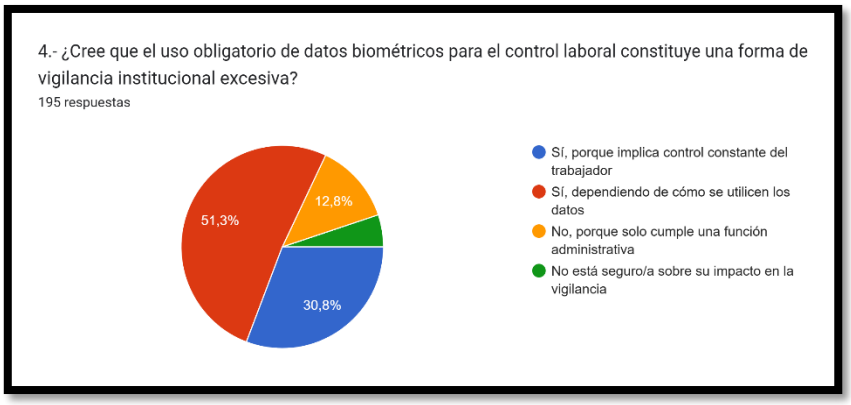
Pregunta 4

¿Cree que el uso obligatorio de datos biométricos para el control laboral constituye una forma de vigilancia institucional excesiva?

Tabla No.4

Opción	Cantidad	Frecuencia
Sí, dependiendo de cómo se utilicen los datos	105	52.5%
Sí, porque implica control constante del trabajador	60	30%
No, porque solo cumple una función administrativa	25	12.5%
No está seguro/a sobre su impacto en la vigilancia	10	5%
TOTAL	**200**	**100%**

Gráfico No. 4



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis:

En lo concerniente a si la obligatoriedad de este registro configura un mecanismo de vigilancia institucional excesiva, el 52.5% de los 200 encuestados adopta una posición condicionada, afirmando que su carácter desmedido depende directamente de cómo se utilicen los datos. Por otro lado, un 30% lo sostiene de manera absoluta al considerar que implica un monitoreo constante del trabajador, lo cual contrasta con un 12.5% que se alinea con la postura de que no existe exceso debido a que cumple estrictamente una función administrativa, y un 5% que no está seguro sobre su impacto en la vigilancia. Estas proporciones abarcan el 100% del espectro de opiniones recabadas.

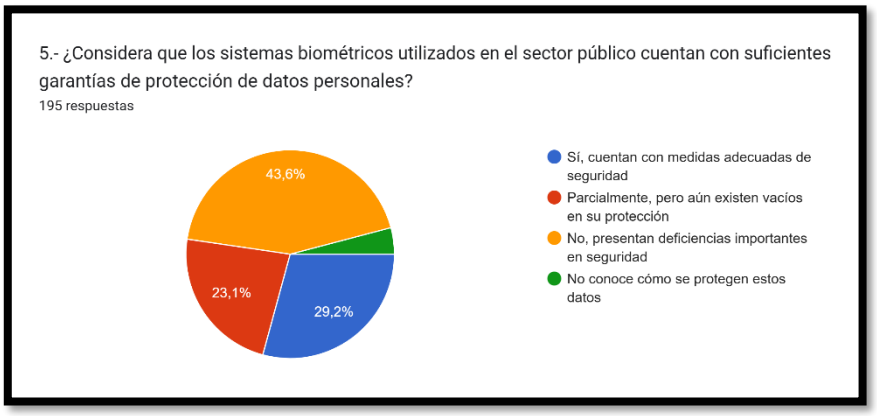
Pregunta 5

¿Considera que los sistemas biométricos utilizados en el sector público cuentan con suficientes garantías de protección de datos personales?

Tabla No.5

Opción	Cantidad	Frecuencia
No, presentan deficiencias importantes en seguridad	90	45%
Sí, cuentan con medidas adecuadas de seguridad	57	28.5%
Parcialmente, pero aún existen vacíos en su protección	45	22.5%
No conoce cómo se protegen estos datos	8	4%
TOTAL	200	100%

Gráfico No. 5



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis:

El análisis de la percepción de seguridad tecnológica demuestra un alto grado de escepticismo, puesto que el 45% de los servidores asegura que los sistemas actuales presentan deficiencias importantes en su protección. A este grupo se añade un 22.5% que califica las garantías como parciales debido a la presencia de vacíos en el sistema. En contraparte, un 28.5% confía en que las medidas implementadas cuentan con protocolos adecuados de seguridad, mientras que un 4% admite desconocer cómo se protegen realmente estos datos, englobando la totalidad (100%) de las 200 respuestas recibidas.

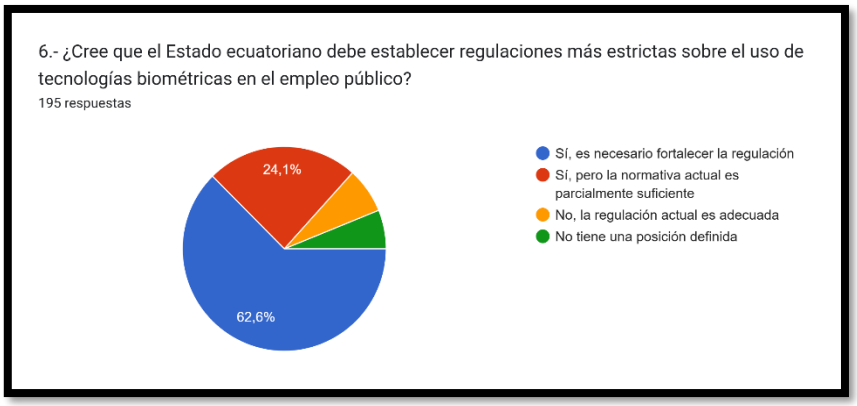
Pregunta 6

¿Cree que el Estado ecuatoriano debe establecer regulaciones más estrictas sobre el uso de tecnologías biométricas en el empleo público?

Tabla No.6

Opción	**Cantidad**	**Frecuencia**
Sí, es necesario fortalecer la regulación	126	63%
Sí, pero la normativa actual es parcialmente suficiente	47	23.5%
No, la regulación actual es adecuada	15	7.5%
No tiene una posición definida	12	6%
TOTAL	**200**	**100%**

Gráfico No. 6



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis:

La necesidad de una intervención estatal normativa expone el consenso más robusto de la investigación. Un contundente 63% de la muestra afirma que es indispensable fortalecer la regulación, demanda que es complementada por un 23.5% que estima que la normativa vigente es apenas parcialmente suficiente. En contraste, solo un 7.5% considera que la regulación actual ya es adecuada, y un 6% declara no tener una posición definida al respecto, lo que en su sumatoria representa el 100% de la visión de los funcionarios sobre el marco legal ecuatoriano.

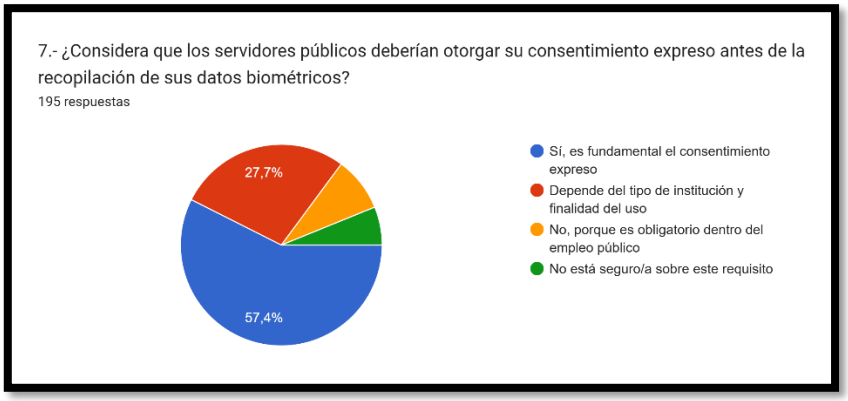
Pregunta 7

¿Considera que los servidores públicos deberían otorgar su consentimiento expreso antes de la recopilación de sus datos biométricos?

Tabla No.7

Opción	**Cantidad**	**Frecuencia**
Sí, es fundamental el consentimiento expreso	115	57.5%
Depende del tipo de institución y finalidad del uso	55	27.5%
No, porque es obligatorio dentro del empleo público	18	9%
No está seguro/a sobre este requisito	12	6%
TOTAL	**200**	**100%**

Gráfico No. 7



Investigador: Fernanda Mishel Guacho Auquilla.

Población: Servidores públicos, Cantón Guaranda, Provincia de Bolívar.

Análisis:

Finalmente, en torno a la exigencia del consentimiento expreso, el 57.5% de los encuestados determina que este requisito es fundamental antes de la recopilación de datos, reflejando una firme defensa de la autodeterminación informativa. Un 27.5% matiza esta postura indicando que el consentimiento debería depender de la naturaleza de la institución y la finalidad del uso. Por el contrario, un 9% sostiene que no es necesario porque es obligatorio dentro de las funciones del empleo público, y el 6% restante afirma no estar seguro sobre este requisito, cerrando de esta forma el 100% del análisis de las 200 encuestas aplicadas.

4.1 Discusión

El presente estudio aborda el análisis jurídico de la implementación de tecnologías de control biométrico en el sector público ecuatoriano, focalizándose en su incidencia sobre el ejercicio del poder administrativo y la potencial vulneración de los derechos humanos de los servidores públicos. La triangulación de la doctrina, la normativa, la jurisprudencia y los hallazgos empíricos derivados de las entrevistas y encuestas, demuestra que el uso de estos sistemas representa uno de los mayores desafíos contemporáneos. Este reto radica en la tensión inherente entre la protección de datos personales sensibles y los límites constitucionales que deben regir la vigilancia institucional.

En el ámbito constitucional, el ordenamiento jurídico ecuatoriano es garantista al reconocer de forma expresa los derechos a la protección de datos personales, la privacidad, la intimidad y la autodeterminación informativa, consagrados tanto en la Constitución de la República como en la Ley Orgánica de Protección de Datos Personales.

Este marco jurídico impone fronteras claras frente al tratamiento indiscriminado de información sensible, no obstante, la investigación tiene una controversia entre la norma y la práctica: la operatividad de las tecnologías biométricas en las entidades públicas aún adolece de vacíos críticos en materia de proporcionalidad, transparencia y salvaguarda efectiva de los derechos fundamentales.

Esta realidad advierte que el crecimiento de mecanismos tecnológicos para la recolección masiva de información amenaza con transformar a las sociedades modernas, socavando la privacidad y la libertad individual, llevado al contexto ecuatoriano, esta advertencia cobra plena vigencia ante la adopción apresurada de controles biométricos como la huella dactilar y el reconocimiento facial por parte de múltiples instituciones públicas.

Estas implementaciones se han ejecutado, en gran medida, al margen de una regulación específica que delimite controles, garantías y estándares para el tratamiento de datos altamente sensibles en el ámbito laboral.

Al respecto, es imperativo reconocer la naturaleza jurídica excepcional de los datos biométricos al permitir la identificación unívoca e irreversible de un individuo, cualquier vulneración o filtración de esta información acarrea daños potencialmente irreparables para el titular, lo que demanda un blindaje jurídico y tecnológico muy superior al de otros datos personales. La tutela de la biometría no es un asunto netamente informático, sino

una manifestación ineludible de los derechos fundamentales en la era digital, intrínsecamente ligada a la esfera de la autodeterminación informativa.

Los hallazgos cualitativos derivados de las entrevistas respaldan esta necesidad de contención normativa, los actores consultados coinciden en que, si bien la administración pública ostenta la potestad de vigilar el cumplimiento de la jornada laboral de la eficiencia institucional, estas facultades no son absolutas, el poder de dirección y control del Estado y el empleador no puede regirse como un justificativo para instaurar modelos de hipervigilancia desproporcionada que lesionen la dignidad, la intimidad y las libertades de los funcionarios.

Esta perspectiva se alinea directamente con la percepción ciudadana, las encuestas aplicadas en el cantón Guaranda revelan una profunda inquietud social frente a los riesgos inherentes a estas tecnologías, por cuanto la postura mayoritaria identifica a los sistemas biométricos como posibles detonantes de una vigilancia institucional intensificada y como amenazas directas a la privacidad. Estos datos empíricos corroboran la hipótesis central de esta investigación: existe un recelo social debidamente fundamentado respecto a los probables excesos del poder administrativo ejecutados a través de herramientas tecnológicas de control.

Adicionalmente, el estudio pone al descubierto una grave deficiencia en las prácticas de transparencia y en la obtención del consentimiento informado. Un sector significativo de la muestra señala que las instituciones omiten comunicar de forma clara la finalidad del tratamiento biométrico, los plazos de conservación, los riesgos subyacentes y las medidas de seguridad adoptadas. Esta problematica5 institucional vulnera frontalmente los principios rectores de la Ley Orgánica de Protección de Datos Personales, en particular los preceptos de licitud, lealtad, transparencia y minimización de datos.

La consolidación de estas herramientas (reconocimiento facial, monitoreo automatizado y autenticación biométrica) advierte una mutación en la dinámica del empleo público, convirtiéndolas en instrumentos de supervisión permanente que alteran el comportamiento humano ante la percepción de un escrutinio incesante. Esto concuerda con el análisis de Lyon (2018), quien describe cómo las sociedades actuales se sumergen de manera progresiva en "culturas de vigilancia" cimentadas en la extracción tecnológica de información y el monitoreo algorítmico de la actividad laboral.

Capitulo V- Conclusiones y Recomendaciones

5.1 Conclusiones

- La presente investigación permite concluir que, durante décadas, el Estado ecuatoriano operó bajo un profundo vacío normativo que facilitó la recolección y el almacenamiento masivo de datos biométricos en el sector público sin ningún tipo de salvaguarda. Al no existir directrices claras sobre el ciclo de vida de la información, las huellas dactilares de los servidores públicos se acumularon de manera indefinida, exponiendo datos catalogados como sensibles a vulnerabilidades sistemáticas. Esta inercia institucional demostró que, históricamente, las entidades públicas priorizaron la eficacia del control administrativo de asistencia por encima de la privacidad y la seguridad digital de sus trabajadores.

- En este contexto, se evidencia una grave paradoja jurídica originada a partir de la Constitución de 2008. Si bien la Carta Magna marcó un hito innegable al reconocer la protección de datos personales como un derecho fundamental autónomo, su eficacia fue prácticamente nula en la cotidianidad institucional

- En este sentido, cuando una institución pública aplica tecnologías de huellas dactilares o de reconocimiento facial sin llevar previamente a cabo una evaluación de impacto y comprobar su conformidad con la Ley Orgánica de Protección de Datos Personales, se incurre en un modo de proceder que puede acabar siendo arbitrario.

- Asimismo, se determina que la filtración masiva de datos evidenciada por el caso Novaestrat en 2019 no fue un incidente cibernético aislado, sino el síntoma más crítico de la anomia legal del país. Esta crisis en cuanto al fracaso estructural en la custodia de las bases de datos estatales confirmó que el poder público asumiera de manera netamente reactiva la urgencia de legislar de forma integral sobre la materia y abandonar su postura de negligencia digital.

5.2 Recomendaciones

- Es indispensable que las instituciones de la Administración Pública implementen protocolos estrictos que regulen el ciclo de vida de los datos biométricos. Para ello, deben diseñar manuales basados en la privacidad desde el diseño que garanticen el principio de minimización y establezcan mecanismos automatizados para la depuración, anonimización o destrucción definitiva de las huellas dactilares una vez que concluya la relación laboral, erradicando así la práctica del almacenamiento indefinido.

- Se recomienda fortalecer procesos de capacitación jurídica y tecnológica dirigidos tanto a servidores públicos como a autoridades administrativas respecto de protección de datos personales sensibles, autodeterminación informativa y límites constitucionales del poder administrativo, con la finalidad de prevenir vulneraciones a derechos fundamentales derivadas del uso indebido de tecnologías biométricas dentro del empleo público ecuatoriano.

- Se recomienda fortalecer el marco normativo relacionado con el uso de tecnologías biométricas dentro del sector público mediante la elaboración de regulación específica que establezca límites claros respecto del tratamiento de datos biométricos sensibles, incorporando mecanismos obligatorios de evaluación de impacto en protección de datos personales, auditorías permanentes de seguridad informática y controles institucionales destinados a garantizar respeto integral de los derechos humanos.

- Se sugiere al Ministerio del Trabajo y a las entidades reguladoras la emisión de directrices obligatorias orientadas a la actualización de los reglamentos internos en las instituciones públicas y privadas. Es necesario que estos instrumentos normativos delimiten con precisión las facultades del empleador, particularmente el *ius variandi* y el poder de control, frente a los derechos digitales de los servidores y trabajadores

Bibliografía

Asamblea Nacional del Ecuador. (2009). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. Registro Oficial Suplemento N.° 52, 22 de octubre de 2009. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Ley-Organica-de-Garantias-Jurisdiccionales-Constitucional_act_marzo_2020.pdf

Datos Personales LAT. (2023). *Ley Orgánica de Protección de Datos Personales Ecuador: principios, artículo 11*. https://datospersonales.lat/ley-datos-personales-ecuador-lopd-registro-oficial-459/

Dirección Nacional de Registros Públicos. (s.f.). *Ecuador cuenta con un proyecto de Ley de Protección de Datos Personales*. Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://www.telecomunicaciones.gob.ec/ecuador-cuenta-con-un-proyecto-de-ley-de-proteccion-de-datos-personales/

Ministerio del Trabajo del Ecuador. (2023). *Normas Generales aplicables al control de las obligaciones del empleador y los procedimientos de inspección*. https://www.trabajo.gob.ec

Juris.pe. (2026). *Los límites al poder de dirección del empleador*. https://juris.pe/blog/ius-variandi-cuales-limites-poder-direccion-empleador/

Lexis Ecuador. (2025, 12 de mayo). *Protección de datos personales en Ecuador: avances, desafíos y debates actuales*. https://www.lexis.com.ec/blog/proteccion-de-datos-ecuador/proteccion-de-datos-personales-en-ecuador-avances-desafios-y-debates-actuales

Ministerio del Trabajo del Ecuador. (2023). *Normas Generales aplicables al control de las obligaciones del empleador y los procedimientos de inspección*. Registro Oficial Suplemento N.° 447, 29 de noviembre de 2023. https://www.trabajo.gob.ec

Orizontel. (2026, marzo). *Ley Orgánica de Protección de Datos Personales: análisis exhaustivo con Reglamento y normativa SPDP vigente*. https://orizontel.ec/guia-lopdp-ecuador/

Primicias. (2021, 25 de mayo). *El camino de Ecuador hacia una Ley de Protección de Datos Personales*. https://www.primicias.ec/noticias/tecnologia/ecuador-ley-proteccion-datos-personales/

SciELO. (2020). *El principio de razonabilidad laboral: los límites a las potestades del empleador en el derecho del trabajo*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122020000200001

Universidad Regional Autónoma de los Andes. (2024). El tratamiento de datos personales en el entorno digital ecuatoriano. https://doi.org/10.56171/episteme.v11i2.412

WIPO Lex. (2017). *Código Orgánico Administrativo: principio de juridicidad, artículo 14*. https://www.wipo.int/wipolex/es/legislation/details/18944

Huerta, I. (2022). Métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(15), 1-17. https://doi.org/10.56 162/transdigital85

ANEXOS

UNIVERSIDAD ESTATAL DE BOLÍVAR
FACULTAD DE JURSPRUDENCIA CIENCIAS SOCIALES Y POLÍTICAS CARRERA DE DERECHO

FORMULARIO DE ENCUESTAS

"TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS"

El estudio busca analizar cómo estas tecnologías son aplicadas en el control laboral, así como las implicaciones que generan en el ejercicio del poder administrativo y en la garantía de derechos fundamentales como la privacidad, la intimidad y la protección de datos personales.

1.- ¿Usted cree que el uso de tecnologías de control biométrico en las instituciones públicas genera un adecuado control administrativo de los servidores públicos, considerando la problemática existente en el manejo y protección de sus datos personales?

Sí, porque permite un control más ordenado del personal, aunque existen riesgos en el manejo de datos

Sí, pero solo si se garantiza una adecuada protección de la información personal

No, porque existen riesgos importantes en la privacidad y uso indebido de los datos

No está seguro/a debido a la falta de información sobre su tratamiento y seguridad

2. ¿Cree que la implementación de sistemas biométricos en el empleo público puede afectar el derecho a la privacidad de los servidores públicos?

Sí, porque puede existir un manejo inadecuado de los datos personales

Sí, pero solo cuando no se informa claramente el uso de la información

No, porque los datos biométricos se utilizan únicamente para control institucional

No, porque existe suficiente regulación que protege la privacidad de los servidores públicos

3.- ¿Considera que las instituciones públicas informan adecuadamente a los servidores sobre el tratamiento y uso de sus datos biométricos?

Sí, existe información clara y suficiente

A veces, pero no de forma completa o transparente

No, generalmente no se informa adecuadamente

No tiene conocimiento sobre esta información

4.- ¿Cree que el uso obligatorio de datos biométricos para el control laboral constituye una forma de vigilancia institucional excesiva?

Sí, porque implica control constante del trabajador

Sí, dependiendo de cómo se utilicen los datos

No, porque solo cumple una función administrativa

No está seguro/a sobre su impacto en la vigilancia

5.- ¿Considera que los sistemas biométricos utilizados en el sector público cuentan con suficientes garantías de protección de datos personales?

Sí, cuentan con medidas adecuadas de seguridad

Parcialmente, pero aún existen vacíos en su protección

No, presentan deficiencias importantes en seguridad

No conoce cómo se protegen estos datos

6.- ¿Cree que el Estado ecuatoriano debe establecer regulaciones más estrictas sobre el uso de tecnologías biométricas en el empleo público?

Sí, es necesario fortalecer la regulación

Sí, pero la normativa actual es parcialmente suficiente

No, la regulación actual es adecuada

No tiene una posición definida

7.- ¿Considera que los servidores públicos deberían otorgar su consentimiento expreso antes de la recopilación de sus datos biométricos?

Sí, es fundamental el consentimiento expreso

Depende del tipo de institución y finalidad del uso

No, porque es obligatorio dentro del empleo público

No está seguro/a sobre este requisito

ANEXOS

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE JURSPRUDENCIA CIENCIAS SOCIALES Y POLÍTICAS CARRERA DE DERECHO

LISTA DE PREGUNTAS DE ENTREVISTA

Interrogante 1: Fronteras del Poder de Dirección vs. Derechos Fundamentales

Desde su experiencia en el libre ejercicio o la magistratura frente a la implementación de sistemas biométricos en el sector público, ¿cuáles considera que son los parámetros esenciales de ponderación para distinguir cuándo el registro tecnológico responde a una facultad organizativa legítima del Estado y cuándo se transforma en un mecanismo de vigilancia lesivo para la esfera íntima del servidor?

Interrogante 2: Tensiones Normativas y Coexistencia Legal (LOSEP y LOPDP)

La normativa de la función pública exige un control estricto de la jornada laboral, mientras que la ley de protección de datos asigna una tutela especial a la información biométrica por su naturaleza sensible. Bajo este escenario, ¿qué nudos críticos o contradicciones normativas percibe usted cuando las instituciones imponen el registro obligatorio sin calibrar las exigencias de idoneidad y necesidad que manda la LOPDP?

Interrogante 3: Vulnerabilidad Tecnológica y Custodia de Información Sensible

Frente al almacenamiento masivo de rasgos biológicos de los servidores públicos en plataformas institucionales, ¿cuáles son las principales debilidades de infraestructura jurídica o técnica que observa en el país para garantizar la seguridad de estos repositorios, y qué nivel de indefensión provoca esto en los funcionarios?

Interrogante 4: Perspectiva de Reforma y Bloque de Constitucionalidad

Frente a las directrices del Sistema Interamericano y las tendencias del derecho comparado que exigen evaluaciones de impacto previas a la vigilancia laboral, ¿estima necesaria incorporar reformas puntuales a la LOSEP o LOPDP para delimitar el uso de la biometría, o considera que la jurisprudencia de la Corte Constitucional es suficiente para guiar a la administración?

EVIDENCIAS

Gráfico 1



Gráfico 2

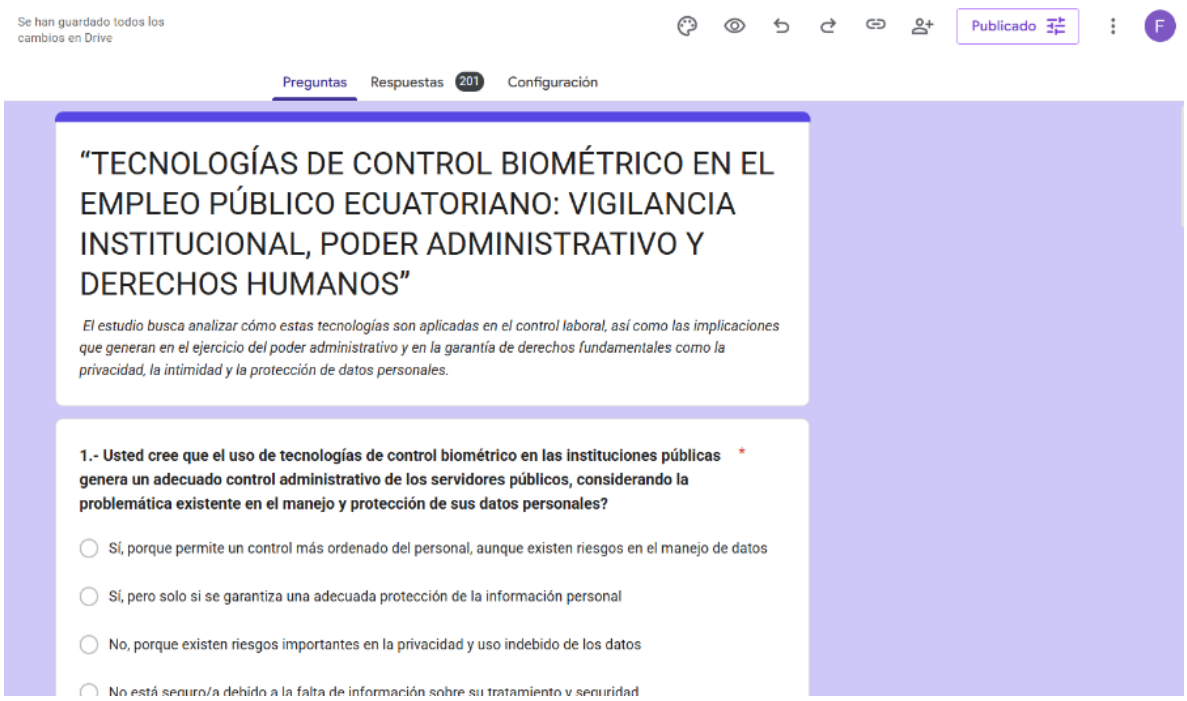
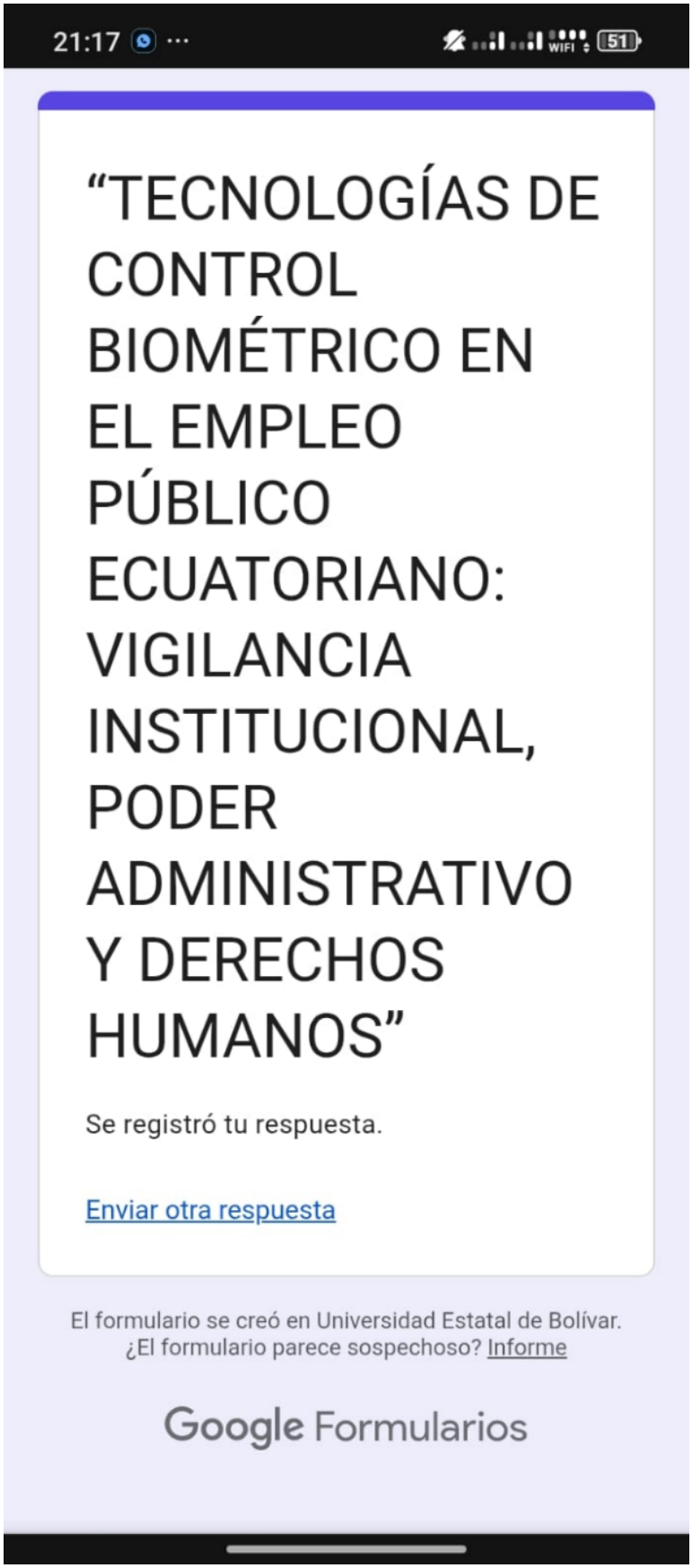


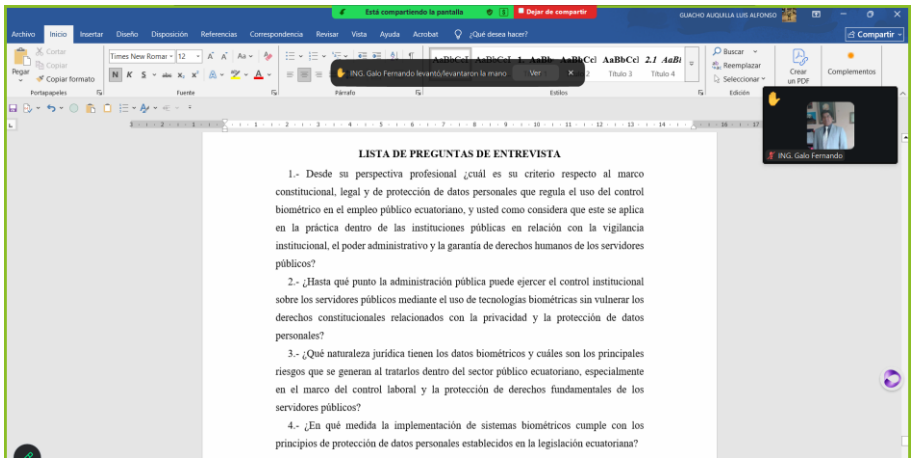
Gráfico 3

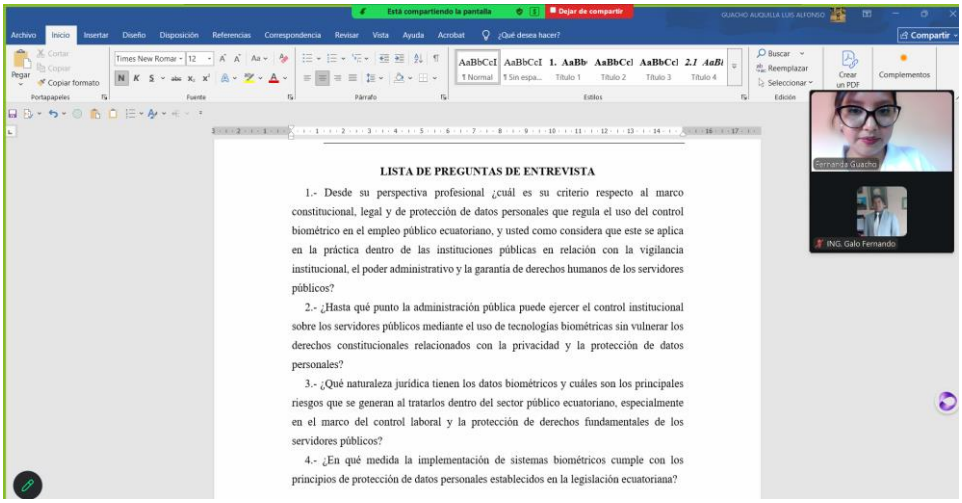

21:17
“TECNOLOGÍAS DE CONTROL BIOMÉTRICO EN EL EMPLEO PÚBLICO ECUATORIANO: VIGILANCIA INSTITUCIONAL, PODER ADMINISTRATIVO Y DERECHOS HUMANOS”
Se registró tu respuesta.
Enviar otra respuesta
El formulario se creó en Universidad Estatal de Bolívar.
¿El formulario parece sospechoso? Informe
Google Formularios

ENTREVISTA

Ing. Galo Fernando Sananay

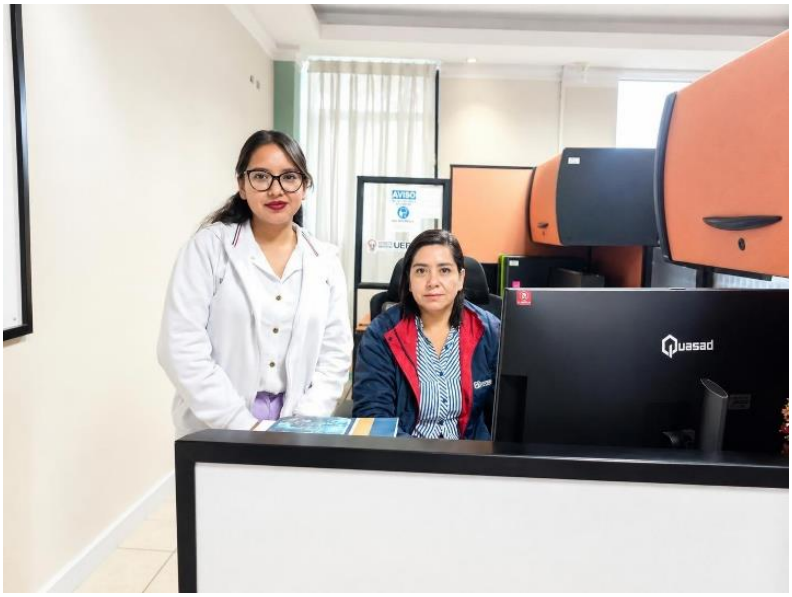
Servidor Público





Lic. Hipatia Ballesteros

Unidad de Redes



Abg. Carola López

Servidora Pública

