**UNIVERSIDAD ESTATAL**

**PENÍNSULA DE SANTA ELENA**

**FACULTAD DE CIENCIAS SOCIALES Y SALUD**

**CARRERA DE DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DE TÍTULO DE ABOGADO**

**TÍTULO:**

# MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025

**AUTORES:**

LUIS ENRIQUE TIRCIO CHÁVEZ

LEONEL DAVID LEÓN GUADAMUD

**TUTORA:**

ABG. KARINA MERCEDES GALLEGOS NORIEGA, M.SC

**LA LIBERTAD – ECUADOR**

**2026**

**UNIVERSIDAD ESTATAL**

**PENÍNSULA DE SANTA ELENA**

**FACULTAD DE CIENCIAS SOCIALES Y SALUD**

**CARRERA DE DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO**

**TÍTULO:**

# MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025

**AUTORES:**

LUIS ENRIQUE TIRCIO CHÁVEZ

LEONEL DAVID LEÓN GUADAMUD

**TUTORA:**

ABG. KARINA MERCEDES GALLEGOS NORIEGA, M.SC

**LA LIBERTAD - ECUADOR**

**2026**

**APROBACIÓN DE LA TUTORA**

**CERTIFICO**

Que he analizado el trabajo de integración curricular con el título **"MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025"** presentado por los estudiantes **LUIS ENRIQUE TIRCIO CHÁVEZ** y **LEONEL DAVID LEÓN GUADAMUD** portadores de cédula de ciudadanía Nº 0924092356 y 1753754314 respectivamente, como requisito previo a optar el título de ABOGADOS, y declaro que luego de haber orientado científica y metodológicamente su desarrollo, el referido proyecto de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la normativa interna, recomendando se inicien los procesos de evaluación que corresponden.

Atentamente

**Abg. Karina Mercedes Gallegos Noriega, M.Sc**

**TUTORA**

**CERTIFICACIÓN DE ANTIPLAGIO**

En mi calidad de Tutora del Trabajo de Unidad de Integración Curricular: "**MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025"**, cuya autoría corresponde a los estudiantes **LUIS ENRIQUE TIRCIO CHÁVEZ** y **LEONEL DAVID LEÓN GUADAMUD** de la Carrera de Derecho, CERTIFICO, que el contenido de dicho trabajo ha sido sometido a la validación en sistema anti plagio COMPILATIO, obteniendo un porcentaje de similitud del 7%, cumpliendo así con los parámetros técnicos requeridos para este tipo de trabajos académicos.


CERTIFICADO DE ANÁLISIS

COMPILATIO LEON-TIRCIO UIC

7% Textos sospechosos

7% Similitudes

< 1% similitudes entre comillas

0% entre las fuentes mencionadas

< 1% Idiomas no reconocidos

3% Textos potencialmente generados por la IA (ignorada)

Nombre del documento: COMPILATIO LEON-TIRCIO UIC.docx
ID del documento: 40f5bbca210c7c9047060f13c2456e186f6759f60
Tamaño del documento original: 511,94 kB

Depositante: KARINA MERCEDES GALLEGOS NORIEGA
Fecha de depósito: 24/10/2025
Tipo de carga: interface
fecha de fin de análisis: 24/10/2025

Número de palabras: 22.535
Número de caracteres: 148.189

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | santaelena.gob.ec \| Política de Protección de Datos Personales<br>https://santaelena.gob.ec/index.php/lista/politica-de-proteccion-de-datos-personales<br>9 fuentes similares | 2% | | Palabras idénticas: 2% (446 palabras) |
| 2 | Marco jurídico.docx \| Trabajo colaborativo 4. Marco jurídico de la audito...<br>Viene de mi grupo<br>3 fuentes similares | 2% | | Palabras idénticas: 2% (367 palabras) |
| 3 | educacion.gob.ec<br>https://educacion.gob.ec/wp-content/plugins/download-monitor/download.php?id=223803&fau...<br>4 fuentes similares | 1% | | Palabras idénticas: 1% (263 palabras) |
| 4 | www.inclusion.gob.ec<br>https://www.inclusion.gob.ec/wp-content/uploads/downloads/2021/03/MIES-2021-004-dc-29-...<br>10 fuentes similares | < 1% | | Palabras idénticas: < 1% (59 palabras) |
| 5 | Documento de otro usuario #94e2ed<br>Viene de de otro grupo<br>7 fuentes similares | < 1% | | Palabras idénticas: < 1% (120 palabras) |

Fuentes con similitudes fortuitas

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | Documento de otro usuario #2223fc<br>Viene de de otro grupo | < 1% | | Palabras idénticas: < 1% (38 palabras) |
| 2 | hdl.handle.net \| El reciente marco de la protección de datos personales (RGPD y ...<br>http://hdl.handle.net/10498/22705 | < 1% | | Palabras idénticas: < 1% (31 palabras) |
| 3 | localhost \| Cobro de los derechos registrales en el registro de la propiedad del Ca...<br>http://localhost:8080/xmlui/bitstream/123456789/15564/1/PUCESA0023-2020.pdf | < 1% | | Palabras idénticas: < 1% (19 palabras) |
| 4 | doi.org \| Protección de datos por diseño y por defecto. Implicaciones legales en el...<br>https://doi.org/10.35381/r.k.v7i1.2427 | < 1% | | Palabras idénticas: < 1% (20 palabras) |
| 5 | Documento de otro usuario #55bb49<br>Viene de de otro grupo | < 1% | | Palabras idénticas: < 1% (20 palabras) |

Atentamente

**Abg. Karina Mercedes Gallegos Noriega, M.Sc**

**TUTORA**

## CERTIFICACIÓN ORTOGRÁFICA Y GRAMATICAL

## CERTIFICO

Que, he realizado la revisión y corrección del Trabajo de Integración Curricular para la obtención del título de **ABOGADOS**, con el tema: "**MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025".** Ha sido desarrollado por los estudiantes de la Carrera de Derecho: **LUIS ENRIQUE TIRCIO CHÁVEZ** y **LEONEL DAVID LEÓN GUADAMUD** de la Universidad Estatal Península de Santa Elena**.**

Que, el trabajo presenta un dominio formal del lenguaje, con expresión clara, coherencia discursiva y solidez interpretativa. Asimismo, garantizando su adecuación a los estándares académicos y formales requeridos.

Por lo expuesto, se expide el presente certificado para que los interesados lo utilicen ante las instancias que correspondan.

Atentamente

Firmado electrónicamente por:

MONICA ISABEL PAREDES CASTRO

Validar únicamente con FirmaEC

Lic. Mónica Paredes Castro, M.Sc.
Magíster en Educación Básica
C.C: 0605353143
Celular: 0969917044

## AUTORÍA DEL TRABAJO

Nosotros, **LUIS ENRIQUE TIRCIO CHÁVEZ** y **LEONEL DAVID LEÓN GUADAMUD**, estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura de Integración Curricular II, declaramos la autoría del presente trabajo de investigación con el título "**MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025",** desarrollado en todas sus partes por las suscritas estudiantes con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE.

Atentamente

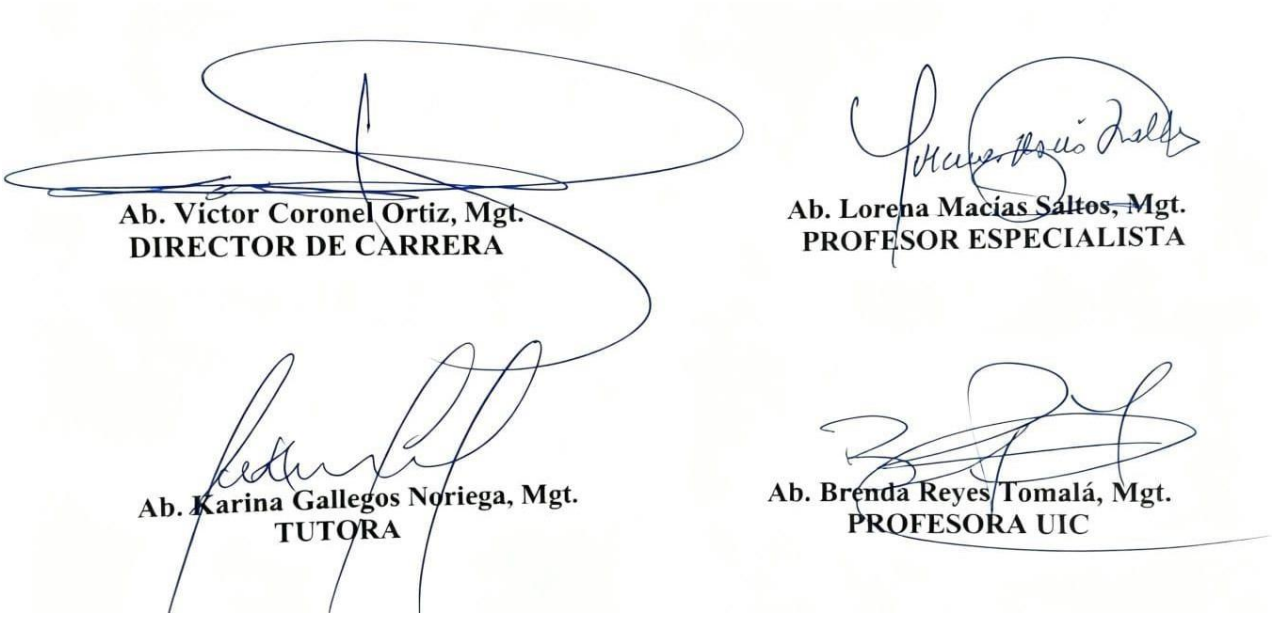
**Luis Enrique Tircio Chávez**

0924092356

**Leonel David León Guadamud**

1753754314

**APROBACIÓN DE TRIBUNAL**



**Ab. Víctor Coronel Ortiz, Mgt.**
**DIRECTOR DE CARRERA**

**Ab. Lorena Macías Saltos, Mgt.**
**PROFESOR ESPECIALISTA**

**Ab. Karina Gallegos Noriega, Mgt.**
**TUTORA**

**Ab. Brenda Reyes Tomalá, Mgt.**
**PROFESORA UIC**

## DEDICATORIA

Dedico este trabajo, con toda mi gratitud a Dios, porque gracias a el obtuve la fuerza y la perseverancia para cumplir mi meta.

A mis padres por ser mi ejemplo para seguir, de ellos aprendí lo que es el esfuerzo, sacrificio y amor incondicional a lo que me proponga tener que culminarlo, gracias por inculcarme buenos principios a soñar y no rendirme.

A mi pequeña familia, que siempre confió en mí y estuvieron en todo este proceso confiando en que lo iba a lograr.

Y a todas las personas que me acompañaron en este duro y difícil camino, y me dieron la apertura para cumplir con este logro tan significativo para mi vida personal y profesional.

**Luis Enrique Tircio Chávez**

Ésta carrera me ha costado mucho esfuerzo y batallas internas, pasé por momentos difíciles como el distanciamiento con mi madre Laura que siempre estuvo conmigo, dándome fuerzas con su amor incondicional, a Maike, José, Aron, Erika y Gabriela y a mí hermana Antonela, gracias por no dejar que me rinda ante las adversidades y siempre recalcar de lo que soy capaz, a Juan Domínguez por ser paz en un mar de caos, y a todos mis maestros en especial a Gabriela Pérez y Lorena Macías que fueron parte de mi formación como una persona luchadora y empática

Este logro es gracias a ustedes que creyeron en mí.

**Leonel David León Guadamud**

## AGRADECIMIENTO

Deseamos expresar nuestro profundo agradecimiento a Dios, quien nos ha concedido la fortaleza y sabiduría necesarias para culminar este trabajo, valoramos sinceramente el apoyo de todas las personas que hicieron posible la realización de nuestra tesis.

Agradecemos de manera especial a nuestra tutora, Abg. Karina Gallegos, por su guía profesional y dedicación constante durante cada etapa de este proceso académico. Reconocemos también la contribución de los docentes de la Universidad Estatal Península de Santa Elena (UPSE), quienes, con su conocimiento y compromiso, nos brindaron las herramientas necesarias para afrontar las exigencias de la investigación.

Extendemos nuestro agradecimiento a los responsables de los departamentos de Talento Humano y del área de Tecnología de la Información y Comunicación de las distintas instituciones de los tres GAD municipales de la provincia de Santa Elena y de la UPSE, su apertura y disposición para colaborar en las entrevistas enriquecieron considerablemente nuestro trabajo, aportando perspectivas fundamentales para el desarrollo de la investigación.

A todos quienes, de una u otra manera, apoyaron y contribuyeron a esta tesis, les reiteramos nuestra gratitud y reconocimiento.

**Luis Enrique Tircio Chávez**

**Leonel David León Guadamud**

**ÍNDICE**

## ÍNDICE DE TABLAS



## ÍNDICE DE ILUSTRACIONES

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA**
**FACULTAD DE CIENCIAS SOCIALES Y LA SALUD**
**CARRERA DE DERECHO**

# MARCACIÓN CON DATOS BIOMÉTRICOS EN EL SECTOR PÚBLICO, 2025

**Autores:** Luis Enrique Tircio Chávez
Leonel David León Guadamud

**Tutora**: Ab. Karina Gallegos Noriega, M.Sc.

## RESUMEN

El presente trabajo de investigación examina sobre la implementación de sistemas de marcación con datos biométricos en el sector público de la provincia de Santa Elena, centrándose en la evaluación de la protección de datos personales según el sistema normativo en Ecuador. El problema central radica en la insuficiencia de mecanismos formales y protocolos adecuados que garantizan la seguridad, confidencialidad y consentimiento informado de los servidores públicos al usar datos biométricos como huellas dactilares y reconocimiento facial para el control de asistencia laboral. El objetivo general es analizar la efectividad de la protección de datos personales en las instituciones públicas, principalmente en los Gobiernos Autónomos Descentralizados Municipales y la Universidad Estatal Península de Santa Elena, con el objetivo de proponer recomendaciones para mejorar prácticas y disposiciones. La investigación se justifica en la necesidad de equilibrar la eficiencia administrativa con la garantía de derechos fundamentales establecidos en la Constitución y la Ley Orgánica de Protección de Datos Personales, dada la alta sensibilidad de la información biométrica y los riesgos asociados a su uso. Las motivaciones para investigar surgen del reconocimiento del incumplimiento normativo y las evidencias empíricas recogidas mediante entrevistas a responsables de talento humano y tecnología, que revelan deficiencias en consentimiento, seguro almacenamiento y normativas internas. Teóricamente, el estudio se fundamenta en principios de protección de datos, anonimización y seudonimización, así como en estándares de seguridad informática del Esquema Gubernamental de Seguridad de la Información (EGSI). Las técnicas principales fueron entrevistas estructuradas, análisis documental y revisión normativa. Como conclusión, se determina que existe un incumplimiento sistemático de las garantías legales para el manejo de datos biométricos, recomendándose la implementación de protocolos específicos, un consentimiento informado estandarizado y auditorías periódicas para asegurar la protección efectiva y el respeto a la privacidad de los funcionarios públicos.

**Palabras claves:** protección de datos, datos biométricos, consentimiento informado, datos sensibles, seguridad de la información.

**ABSTRACT**

This research paper examines the problem of implementing biometric fingerprinting systems in the public sector in the province of Santa Elena, focusing on the evaluation of personal data protection under Ecuador's regulatory system. The central problem lies in the lack of formal mechanisms and adequate protocols that guarantee the security, confidentiality, and informed consent of public servants when using biometric data such as fingerprints and facial recognition for work attendance monitoring. The overall objective is to analyze the effectiveness of personal data protection in public institutions, mainly in municipal decentralized autonomous governments and the Peninsula de Santa Elena State University, with the aim of proposing recommendations to improve practices and provisions. The research is justified by the need to balance administrative efficiency with the guarantee of fundamental rights established in the Constitution and the Organic Law on Personal Data Protection, given the high sensitivity of biometric information and the risks associated with its use. The motivations for conducting this research arise from the recognition of regulatory non-compliance and empirical evidence gathered through interviews with human resources and technology managers, which reveal deficiencies in consent, secure storage, and internal regulations. Theoretically, the study is based on principles of data protection, anonymization, and pseudonymization, as well as on the IT security standards of the Government Information Security Scheme (EGSI). The main techniques used were structured interviews, document analysis, and regulatory review. In conclusion, it is determined that there is a systematic breach of legal guarantees for the handling of biometric data, recommending the implementation of specific protocols, standardized informed consent, and periodic audits to ensure effective protection and respect for the privacy of public officials.

**Keywords:** data protection, biometric data, informed consent, sensitive data, information security.

# INTRODUCCIÓN

La investigación se estructura de manera integral para evaluar el problema de la marcación con datos biométricos en el sector público, pasando desde el planteamiento teórico y normativo, hasta el análisis metodológico y resultados prácticos, por lo que se busca ofrecer una visión clara y ordenada que permita comprender el entorno, la fundamentación legal y técnica, la metodología aplicada, y finalmente, el análisis profundo de los datos recolectados.

El primer capítulo presenta el planteamiento del problema, donde se detalla la situación actual de la implementación de sistemas de marcación biométrica en las diversas instituciones públicas de la provincia de Santa Elena, haciendo un énfasis en la relevancia de la protección de datos personales sensibles que manejan estos sistemas. Se evidencia la problemática concreta que enfrenta el sector público al no contar con protocolos claros para el manejo seguro de estos datos, generando riesgos en el consentimiento informado, almacenamiento y uso, lo que puede derivar en vulneraciones a los derechos fundamentales. Asimismo este capítulo expone los antecedentes normativos y empíricos relacionados con el uso de biometría en la administración pública y se delimita el problema de investigación con claridad, en este espacio se definen el objetivo general y los objetivos específicos con base en la necesidad de evaluar la efectividad de las políticas y prácticas actuales, además, se incluye la justificación que argumenta la importancia social y jurídica de la investigación, y se exponen las motivaciones personales y académicas que impulsan este estudio, destacando la necesidad de promover un equilibrio entre eficiencia administrativa y los derechos a la privacidad.

El segundo capítulo se enfoca en el marco teórico y conceptual, donde se revisan y analizan las teorías fundamentales sobre protección de datos personales, anonimización y seudonimización, además del análisis del marco jurídico vigente, incluyendo la Constitución del Ecuador y la Ley Orgánica de Protección de Datos Personales, también se incorporan conceptos claves y estudios previos que fundamentan la investigación, así como indicadores relevantes para evaluar la gestión y protección de datos biométricos.

En el tercer capítulo se desarrolla el marco metodológico, que explica el enfoque cualitativo y descriptivo, el modelo de investigación, la población del estudio, y las técnicas e instrumentos de recopilación de información, como entrevistas y análisis documental, esta sección aclara cómo se operacionalizan las variables y se aplican métodos de análisis que garantizan la validez y confiabilidad de los resultados.

Finalmente, el cuarto capítulo presenta el análisis de resultados, donde se interpretan los datos recolectados y se evalúa el grado de cumplimiento de las normativas de protección de datos en las instituciones investigadas. Se identifican las principales deficiencias, fortalezas y diferencias, para luego discutir con base en la teoría y el marco normativo, esta parte culmina con conclusiones y recomendaciones orientadas a mejorar la gestión de los datos biométricos en el sector público.

# CAPÍTULO I

# PROBLEMA DE INVESTIGACIÓN

## 1.1. Planteamiento del problema

El uso creciente de la tecnología biométrica como un mecanismo de marcación laboral destaca una necesidad de equilibrio entre la tecnología de marcación mediante la biometría y el valor a la protección de los datos personales, la mismo que requiere de transparencia ante una regulación e información digital. De acuerdo con Innovatrics (2023) “los sistemas de identificación biométrica son cada vez más populares en el mundo actual, ofreciendo una capa adicional de seguridad y precisión en diversas aplicaciones” (p. 1).

Globalmente se ha incrementado manera oportuna las nuevas formas de tecnología, estas que ayudan de cierto modo a facilitar el reconocimiento y la información, ya sea, proporcionada, almacenada o distribuida. La implementación de la biometría es una tecnología de identificación que se ha implementado en muchos países con el fin de almacenar y registrar la información de los usuarios, ya que la misma es autenticar con las características físicas de las personas lo que hace un perfil único de ellos, a su vez con la intención que estas no permitan transferirse, replicarse o mucho menos falsificarse, porque de cierto modo este goza de su exclusividad. Una de las formas más eficaces para las empresas de tener el registro de sus empleados son el uso de la marcación con huella dactilar, se considera como uno de los métodos más seguros para signar un registro único, no obstante, este tiene un margen de error mínimo, otra de las formas de valerse con los datos biométricos para los registros es el reconocimiento facial, la cual es la forma más moderna de inducción en las empresas.

Dentro del campo laboral como marcación de asistencia lo implementado en los últimos años abarca una serie de recursos tecnológicos que ayudan hacer eficiente esta tarea de regular datos para un almacenamiento interno de la empresa que lo practica, el control de

asistencia esta idealizado para comprender los turnos de trabajo de cada empleado este que necesita de un perfil único de cada persona en marcación biométrica.

> En el control de asistencia, está el reloj control biométrico que utiliza reconocimiento facial para realizar la marcación, el cual se basa en un dispositivo electrónico que reconoce el rostro de cada colaborador y registra de esa forma tanto el comienzo como el fin de sus turnos de trabajo (Miranda, 2024).

En Ecuador, se regula la protección y seguridad de datos personales de todos los ciudadanos en el país, de conformidad con el artículo 66, numeral 19 de la Constitución, que decreta lo siguiente: "la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o por el mandato de la ley" (Constitución de la República del Ecuador, 2008). Es ineludible que exista el consentimiento de la persona titular ya que la misma debe entender que su información personal será manipulada por una tercera persona.

La protección de datos personales es decisiva a manera de aplicación y preservación de este en la sociedad que estamos presente, según Solove (2008) en su libro titulado: Entendiendo a la privacidad "ofrece un panorama completo de las dificultades que plantean los debates sobre la privacidad y, en última instancia, ofrece una solución sugerente" (pág. 9). Es decir, que no existe una interpretación única de lo que es la privacidad ya que de esta desprenden un sin número de variables evidenciadas en el libro. Además, describe como se encuentra una solución interesante, marcando este factor como un entendimiento más práctico de aquello, las relaciones que conformar la privacidad tiene una brecha de similitudes. Su teoría busca en su poder entrelazar aspectos culturales y llevar a cabo la investigación de como el desarrollo de conocimientos de cada una ha hecho diferente la forma de cómo podemos apreciar la privacidad a lo largo del tiempo.

A medida que, la tecnología avanza en nuestra sociedad la recolección de datos es más ágil y la torna fácilmente accesible, Solove (2008) en su libro, utiliza ciertas fuentes de apoyo de diferentes disciplinas para crear un marco referencial, el mismo que ayuda a entender con mayor argumentación y amplitud la privacidad, entre ellas son: la vigilancia, el robo de identidad, la extracción de datos y la más importante que es la participación del Estado en

estas situaciones. Desde un punto más relacionado en la Constitución y leyes que deben amparar la distribución de aquel como antes mencionado es el complejo del consentimiento de la persona para que esta de apertura a este tipo de función que es el almacenamiento a un tercero en este caso por obligación laboral entre muchos aspectos que pueden limitar la privacidad.

La Superintendencia de Protección de Datos Personales, (2024) en el Registro Oficial N.º 683 del 14 de noviembre del 2024 mediante el oficio No. SPDP-IRD-2025-0031-O, solicita a las empresas que analicen el uso de datos biométricos para controlar la asistencia de sus empleados de forma regulada, este requerimiento enfatiza la necesidad de medidas de seguridad sólidas para proteger la privacidad de los datos sensibles, exigiendo un manejo cuidadoso y protegido con el fin de mitigar riesgo y evitar el uso indebido de los datos.

Según el Diario Expreso (2025) toma como medida que "la entidad encargada de proteger la privacidad de los ciudadanos ha señalado que esta práctica podría ser vista como excesiva e innecesaria, compromete principios fundamentales de protección de la información, en particular la privacidad de los empleados". Por parte de la empresa la autoridad enfatiza que los datos biométricos se consideran de una forma exclusiva como información delicada, según la Ley Orgánica de Protección de Datos Personales, lo que hace relevante que solicite una protección especial, sin embargo las empresas se cuestionan ante la garantía de este nivel de protección adecuadamente en el mismo entorno laboral que pueda suponer un riesgo para los empleados al momento que esta medida sea desarrollada, el organismo responsable de la protección de aquel se cuestiona a su vez al grado de convertirse en un vacío jurídico dentro del país, en el sentido de advertencia por medio de un consentimiento obtenido puede no ser únicamente libre.

De acuerdo con la Ley Orgánica de Protección de Datos Personales cuyo ámbito de aplicación se dirige a todo el territorio ecuatoriano, contiene una serie de disposiciones que regula tanto en el ámbito privado y público el manejo y custodia de los datos personales de los ciudadanos, en este sentido para efecto de este estudio se observa el comportamiento de esta problemática en el sector público de la provincia de Santa Elena.

El registro de datos biométricos empleada en el sector público de la provincia de Santa Elena tiene un impacto significativo en el ámbito laboral, este permanentemente busca la marcación oportuna y rápida de sus empleadores en el horario laboral tanto en los 3 GAD

Municipales de Santa Elena, Libertad y Salinas como en la Universidad Estatal Península de Santa Elena (UPSE). Estas instituciones emplean esta actividad de registro con datos biométricos, huella dactilar, reconocimiento facial y lector QR donde debe abarcar el consentimiento directo de sus empleados para el conocimiento del registro de sus datos únicos y la protección.

El Gobierno Autónomo Descentralizado Provincial de Santa Elena reconoce a los titulares de datos personales el acceso y rectificación al tratamiento que se realice sobre sus datos, mediante los mecanismos y procedimientos definidos por la institución (GADPSE, 2023). En la provincia de Santa Elena los sectores públicos funcionan correctamente, pero sus empleadores como principal función deben impartir el conocimiento de la práctica a sus empleados sobre el almacenamiento y manipulación de sus datos únicos registrados con la actividad del registro biométrico mediante la huella dactilar, reconocimiento facial y lector QR al momento de su ingreso, estas mismas que son almacenadas dentro de un núcleo de información corporativa y cuál es la forma de garantía que brinda el Estado para protegerlos.

### 1.2. Formulación de la pregunta de investigación

¿Cómo la implementación de sistemas de marcación con datos biométricos en el sector público de la provincia de Santa Elena garantiza del derecho a la protección de datos personales?

### 1.3. Objetivos de la investigación

#### 1.3.2. Objetivo general

Analizar el uso de marcación con datos biométricos en el sector público, mediante la revisión de su implementación en la provincia de Santa Elena en los GAD Municipales de Santa Elena, Libertad, Salinas y la Universidad Estatal Península de Santa Elena (UPSE), para la evaluación de su efectividad en el derecho de protección de datos personales.

#### 1.3.2. Objetivos específicos.

1. Evidenciar el uso de marcación de datos biométricos en el sector público, evaluando su implementación en los procesos administrativos para considerar la protección de datos de los ciudadanos en las entidades del sector público provincia de Santa Elena.
2. Identificar las diferentes medidas de protección y garantías que se brindan a la protección de datos personales, mediante la marcación de la biometría con huella

dactilar y reconocimiento facial en el sector público de la provincia de Santa Elena.

3. Examinar las implementaciones legales y éticas del uso de la marcación con datos biométricos en el sector público, comparando el enfoque directamente en la privacidad y derechos de los ciudadanos conforme al artículo 66, numeral 19 de la Constitución del Ecuador, para garantizar su aplicabilidad.

### 1.4. Justificación

La marcación con datos biométricos en el sector público es una realidad inevitable, un mecanismo eficaz y casi infalible para controlar la asistencia y agilizar los procesos administrativos, no obstante al igual que toda tecnología de considerable alcance su filo corta en ambas direcciones, tras la eficiencia fría del sistema se esconde una cuestión más delicada: el equilibrio entre la seguridad institucional y la privacidad de quienes día tras día dejan huella literal y figurada en los registros de su lugar de trabajo.

El consentimiento de una persona al aceptar de cierta forma accede a diferentes tipos de acciones, nace de la práctica de ser consientes con las decisiones, en el tema laboral dentro de la protección de datos únicos debe prevalecer honestidad y el valor de garantizar una plena administración de información de todos los empleados, como referencia de una respaldo óptimo y muestra de consentimiento informado lo evidenciamos en los contratos, los que gozan de mostrar cláusulas y formas de extinción, dejando claro el ejercicio de consentimiento al que en este caso el colaborador se debe sostener sobre la protección de los datos únicos.

Para comprender la magnitud del problema, conviene examinar primero la naturaleza misma de los datos biométricos. Son códigos únicos e irrepetibles, sellos de identidad más precisos que una firma y más definitivos que un documento de identidad. No es casualidad que la Constitución del Ecuador en su artículo 66, numeral 19, sea clara al respecto de qué ningún dato personal puede ser recolectado sin el consentimiento de su titular o sin el respaldo de una orden legal. La Ley Orgánica de Protección de Datos Personales (2021) en su artículo 4 es aún más taxativa al catalogarla como “datos sensibles”, sujeta a estrictas normas para su recolección y almacenamiento. En definitiva, lo que se registra en un sistema biométrico no es un simple código de acceso; es la esencia digitalizada de una persona.

En Santa Elena, la disputa entre la eficiencia y la protección de la privacidad se desarrolla en los pasillos de varias instituciones públicas, la implementación de sistemas como reconocimiento facial, huella dactilar y código QR para registrar la asistencia del personal en instituciones como los Gobiernos Autónomos Descentralizados GAD municipales y la Universidad Estatal Peninsular de Santa Elena (UPSE) presenta interrogantes sobre la seguridad y privacidad de los datos biométricos obtenidos.

La Superintendencia de Protección de Datos Personales ha dado la voz de alarma, alertando sobre los riesgos de la recolección de datos biométricos en forma masiva y recordando que la acumulación descontrolada de información puede derivar en violaciones a la privacidad de los trabajadores.

### 1.5. Idea a defender

Los sistemas de marcación con datos biométricos implementados en las instituciones del sector público de Provincia de Santa Elena no garantiza la protección de datos personales de los servidores públicos, en el marco de las reglas establecidas de la Ley Orgánica de Protección de Datos.

### 1.6. Variables

#### 1.6.1 Variable independiente

- Sistemas de marcación con datos biométricos en el sector público.

#### 1.6.2 Variable dependiente

- Protección efectiva de los datos personales sensibles.

# CAPÍTULO II

# MARCO REFERENCIAL

## 2.1 Marco teórico

### 2.1.1 Protección de datos personales a la luz del desarrollo

La protección de datos se refiere a los derechos de las personas sobre sus datos. Se deben considerar obligaciones legales y éticas al compartir información personal.

Los datos personales incluyen cualquier información que identifique a una persona, como teléfono, edad o dirección. Un controlador puede designar un procesador de datos, pero sigue siendo responsable de la seguridad de la información recopilada.

> Los datos personales se refieren simplemente a los registros u otra información que por sí sola o vinculada con otros datos, puede revelar la identidad de una persona viva, así, por ejemplo, puede utilizar números en lugar de nombres como identificadores en una encuesta, pero si mantiene otro registro vinculando esos números a los nombres reales, se considera que cada registro contiene información personal (CEPAL, 2024).

Proteger la privacidad y seguridad de los datos personales es importante, ya que la información puede parecer como anónima o no identificativa puede convertirse en personal si se combina con otros datos. El ejemplo que menciona CEPAL (2024), de la encuesta con números en lugar de nombres es ilustrativo de como la información puede ser considerada incluso si no es directamente identificativa. Si se mantiene un registro que vincula esos números a nombres reales se considera que cada registro contiene información personal y únicos.

Las organizaciones y entidades datos deben tener en cuenta la posibilidad de la información aparentemente anónima pueda ser vinculada con otros datos para revelar la identidad de la persona esto requiere un monitoreo constante de los datos y la implementación de medidas de seguridad adecuadas para proteger la privacidad de las personas.

En la actualidad la cantidad de datos que se generan y se comparten es enorme, la capacidad de vincular datos de diferentes fuentes y la creciente de sofisticación de los algoritmos de análisis de datos hacen que se cada vez más importante proteger la privacidad y seguridad de los datos personales.

#### 2.1.1.1. Antecedente comparativo de la protección de datos sensibles

Durante décadas la protección de datos sensibles ha sido un tema de interés, que ha cobrado mayor interés en la actualidad. La creciente capacidad de almacenar, recopilar y analizar grandes cantidades de datos genera preocupaciones sobre la privacidad y seguridad de la información personal.

La protección de datos sensibles varía entre países y regiones, algunos países han implementado leyes y normas estrictas para proteger los datos sensibles, mientras otros han adoptados enfoques más permisivos.

> El examen del tratamiento normativo en materia de protección de los datos personales dentro del derecho europeo corresponde centrarnos en el caso del derecho español, teniendo en cuenta que sus leyes son las que modelan la legislación dentro del contexto normativo hispano, en especial la legislación de América del Sur, incluyendo el caso chileno (Sanz, 2016, p. 328).

La influencia del derecho español en la protección de datos personales tiene efectos significativos para la privacidad y la seguridad de las personas, porque la normativa hispana sugiere que existen similitudes y patrones comunes en la regulación de la protección de datos en los países de América del Sur. Esto puede facilitar la cooperación y el intercambio de experiencias entre estos países que pueden ser beneficiosos para mejorar la protección de datos sensibles en la región.

##### 2.1.1.1.1. Principios rectores jurídicos en la protección de datos personales

La protección de datos se refiere a los derechos de las personas cuyos datos de forma conjunta se almacenan, para mantenerlos y procesarlos, este depende de una serie de información recabada en el desarrollo de la transformación hacia un órgano activo, si la investigación involucra personas se debe considerar como autor para conocer y considerar sus obligaciones legales, el controlador de datos determina el propósito de los mismos, su manejo y su manipulación para tener un fin, el controlador de los datos se puede visualizar de diferente forma, como una persona, institución o empresa.

Los principios de protección de la protección de datos personales aluden como prioridad la privacidad y derecho individual que da garantía el control sobre la información personal, tiene como finalidad tener en cuenta que los datos personales pueden dividirse entre datos sensibles estos son los que dan exclusividad a los rasgos de una persona y esta misma protege la salud la religión la etnia entre otros.

De acuerdo con Reglamento del Parlamento Europeo (2016) La Unión Europea adoptó el Reglamento General de Protección de Datos (GDPR) con el objetivo de reforzar y unificar la protección de los datos personales de sus ciudadanos, esta normativa fue aprobada en conjunto por las principales instituciones europeas que entró en vigor el 25 de mayo de 2018. El GDPR de la Unión Europea impone sanciones relevantes a quienes no cumplan con sus disposiciones, las multas pueden llegar hasta 20 millones de euros o el 4% de la facturación global anual de la empresa infractora, aplicándose la cantidad más alta.

La normativa, presenta retos considerables para las empresas pequeñas y medianas, que deben adaptarse a los requisitos de protección de datos y seguridad, esto puede afectar negativamente en la confianza de los usuarios y la reputación empresarial. Para mitigar estos riesgos es esencial que las empresas implementen medidas efectivas de seguridad de datos, este recurso está diseñado para ayudar a los propietarios y gerentes de empresas pequeñas y medianas a resolver problemas específicos relacionados con la protección de datos, aunque no reemplaza el asesoramiento legal, puede ayudarle a comprender mejor la normativa y enfocar sus esfuerzos para adaptarse a la protección estipulada en la ley. También ofrece alternativas y formas de precaución ante los riesgos que pueden surgir cuando los usuarios comparten información personal en las empresas para desarrollar sus actividades laborales.

La ley sobre la seguridad de datos personales abarca cientos de páginas con nuevos requisitos para las organizaciones de todo el mundo, con el objetivo de establecer una relación de protección de datos entre organizaciones que trabajan con la misma finalidad de seguridad, aunque fue desarrollada y aprobada por la Unión Europea, esta normativa impone obligaciones a las organizaciones en cualquier lugar del mundo que envíen o recopilen datos relacionados con personas de la Unión Europea, como se ha señalado “el objetivo principal del Reglamento General de Protección de Datos es dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la Unión Europea” (PowerData, 2025), las regulaciones

que entraron en vigor en 2018, establecen multas graves para quienes violenten los estándares de seguridad.

La Unión Europea ha sido pionera en la protección de datos personales, en 1995 se estableció los principios de protección de datos con el objetivo de proteger los derechos y libertades de las personas, fomentar la confianza entre ellas y dar seguridad a la economía digital, unificando las normativas de protección de datos. Entre los principios clave de la protección de datos se encuentra "uno de los pilares del Reglamento General de Protección de Datos RGPD es el principio de privacy by design, que exige que la protección de datos personales esté integrada desde el diseño inicial de cualquier sistema tecnológico" (Saúco, 2025), esto significa que el procesamiento de los datos debe realizarse con transparencia y consentimiento de las personas, además los ciudadanos tienen derechos específicos en relación con la protección de sus datos personales.

En el ámbito de los avances tecnológicos y el desarrollo en la Unión Europea, se han planteado innovadores retos para la seguridad de los datos personales en los últimos años, el rápido avance en la recopilación y el intercambio de datos personales ha llevado a un almacenamiento exponencial a escala mundial, aunque cada vez más personas están dispuestas a compartir sus datos personales, es fundamental tener en cuenta que estos datos pueden convertirse en información sensible.

La tecnología ha entrado en una era de transformación que exige promover la protección de la economía digital y garantizar un alto nivel de protección de los datos personales, esto implica equilibrar la libertad de desarrollo de los datos con la necesidad de proteger la privacidad y seguridad de las personas, en estas circunstancias los datos personales utilizados con fines de investigación policial deben ser manejados con cuidado y separados de otros usos.

Las autoridades de cada Estado miembro tienen la necesidad de intercambiar datos en el marco de la lucha contra la delincuencia transnacional y el terrorismo, lo que requiere medidas de protección efectivas para garantizar la seguridad de la ciudadanía, en este sentido la protección de datos personales es fundamental para mantener la confianza en la economía digital y prevenir abusos.

Dentro de este entorno del desarrollo de datos personales en la tecnología es fundamental tener en cuenta que existen normas claras y específicas sobre la protección de datos

personales a escala de la Unión Europea las mismas que son coherentes para poder tener una descripción de cada una de las normativas para mejorar la cooperación entre las autoridades que intervienen en esta potencia.

Los datos personales se han convertido en un derecho fundamental de las personas en virtud del derecho de la Unión Europea, este país reconoce este derecho en el Tratado de Funcionamiento y en la Carta de los Derechos Fundamentales. Además, es importante en el ámbito de la seguridad personal, ya que los datos personales de un individuo pueden proporcionar acceso a una gran cantidad de información almacenada, esta información puede incluir registros previos que se actualizan cada vez que una persona es sometida a un registro biométrico o a alguna otra forma de intervención.

> La protección de los datos personales y el respeto de la vida privada son derechos europeos fundamentales. El Parlamento Europeo ha insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada (Maciejewsk, 2025).

Según el Reglamento General de Protección de Datos de la Unión Europea, este reglamento se refiere a la seguridad de las personas en lo que respecta al procedimiento de manipulación de los datos personales y a la libertad que tienen en el desarrollo de estos, en su texto se incluyen las correcciones de errores que fueron publicadas en el Diario Oficial de la Unión Europea en el año 2018. La implementación del Reglamento General de Protección de Datos Personales fue una etapa fundamental para dar importancia al fortalecimiento de los derechos de las personas en la actual era digital, con el fin de facilitar el acceso a la información y proteger los derechos de los individuos, este reglamento también tiene como objetivo facilitar las actividades comerciales, aclarando explícitamente las normas para las empresas públicas y privadas que necesitan obtener datos de sus clientes y empleados, así como para los organismos públicos en el mercado único digital.

#### 2.1.1.1.2 Evolución histórica en Ecuador como forma de principio fundamental en la protección de datos personales

El Ecuador estaba entre los países que adoptó como ley fundamental la protección de datos personales el cual se basó en el ideal de la Unión Europea el mismo, que ha sido referente para algunas reformas legales dentro del país. Cabe recalcar que en Ecuador ya existía una

ley de protección de datos más no alternativas y planes de protección ante emergencias de situaciones de datos personales en el país.

En el desarrollo del país se ha buscado tener como prioridad la seguridad de los ciudadanos y con estos la información de cada uno de ellos el país ha atravesado por muchos problemas sociales de diferentes situaciones pero en la ola de la tecnología de los últimos años estos han llegado como un impacto de facilidad de obtención de información en nubes de tecnología y de almacenamiento de la misma haciendo factible y recomendable su uso para agilizar tiempos de búsqueda dentro de investigaciones fundamentales.

De acuerdo con Rosas & Pila (2023) detallan que "actualmente, los datos personales representan un bien altamente valorado no solo por las instituciones públicas o privadas que operan legalmente", las empresas públicas y privadas han adoptado ciertas medidas de seguridad para poder tener un almacenamiento y base de datos del desarrollo de sus actividades económicas digitales pero también han implementado la marcación de registro de sus empleados en el tema de asistencia a sus horarios laborales. Las diferentes mecanismos de marcación de asistencia que han adoptado estas empresas públicas y privadas y el más usual actualmente son los registros biométricos estos ayudan a la obtención de forma rápida y eficaz para un control de información en tiempo real dejando este un historial de información de la persona que marca la misma, pero actualmente se conoce que no es el mejor uso para una persona facilitar sus datos personales previo consentimiento de éste se debe dar a conocer las implicaciones sociales que tiene el uso de datos personales tal y como menciona la definición:

> Los datos biométricos, tales como la huella dactilar, el reconocimiento facial o del iris, se consideran datos personales sensibles bajo la LOPDP. Esto implica que su tratamiento está sujeto a un mayor nivel de protección y sólo puede realizarse bajo circunstancias específicas. (Bustamante Fabara, 2025)

La biometría que usa huellas dactilares y reconocimiento facial es uno de los procedimientos más sensibles ya que los datos son de ultra autenticidad de la persona, asumiendo una originalidad única, "este tipo de datos que recogen una característica física intransferible es en efecto un dato personal al amparo de la Ley Orgánica de Protección de Datos Personales (LOPDP), que incluso lo establece como un dato sensible" (ECIJA, 2022) , el procedimiento que desarrolla la base de datos en su almacenamiento es de carácter sensible ya que en la

base de datos deja un historial único de cada persona que registra su identidad, el almacenamiento de datos sensibles llega a una base de datos donde es fundamental proveer la seguridad de cada uno de la información guardada.

> Las huellas dactilares son una de las características biométricas más antiguas y fiables utilizadas para la identificación de personas. Durante siglos, las huellas dactilares han sido reconocidas por su singularidad, lo que las convierte en un método de identificación altamente seguro. (Castillo, 2024)

Cuando se configura un dispositivo para reconocer nuestra huella dactilar, el dispositivo escanea y almacena un patrón único de las características personales, si hay una coincidencia con el aparato biométrico se desbloquea y podemos acceder a él. En este caso es la característica utilizada para identificar los dactilares únicos lo que hace que sea muy difícil de falsificar o duplicar la biometría funciona basándose en cuatro pasos biométricos estás son la extracción característica, comparación, coincidencia, y verificación. Como el reconocimiento facial, donde se captura con datos biométricos previamente autenticados con características del usuario para el reconocimiento del rostro, se pueden utilizar técnicas de reconocimiento de voz, en la que se mide la frecuencia el tono y el acento, el dispositivo que actualmente está en el alcance de muchas instituciones es un desarrollo para la tecnología sin embargo es un proceso delicado al momento de implementarlo.

La identificación por huella dactilar es sin duda una tecnología más madura utilizada en todo el mundo, como características contribuyentes tiene la precisión de su identificación y seguridad, también hoy en día se pueden adquirir de una forma más fácil ya que en el mercado el desarrollo tecnológico fue incrementando en todos sus sistemas operativos. Se han conseguido velocidades de comparación elevada gracias al método de capacidad de cálculo incluso si la base de datos es amplia, su desventaja fundamental es el deterioro de las huellas dactilares con la edad de las personas, también es con personas que trabajan con químicos y sus huellas dactilares de alguna forma sufren de alguna anomalía, dado que la huella tiene muchos usos como en la presente investigación que es la marcación de asistencia al horario laboral, está ola de tecnología donde se encuentra aún en desarrollo de autenticidad nos abre la brecha a miles de ventajas y desventajas. .

El sistema biométrico de reconocimiento facial es la segunda técnica más utilizada como actividad de marcación, “la tecnología de reconocimiento facial no es nada nuevo. Ha

evolucionado en las últimas décadas, pasando de ser un concepto de ciencia ficción a formar parte integral de nuestra vida cotidiana, protegiendo teléfonos, hogares, cuentas y empresas" (Cheon, 2025), entre sus principales ventajas tenemos que se puede utilizar a distancia y no necesita un manejo del usuario su ejercicio es autónomo cuando comienza a procesar, por lo que no requiere la colaboración del usuario se puede emplear en sistemas de vigilancia, y por otro lado es comúnmente es aceptado por las personas y esto está influido por las redes sociales. El mismo es idóneo para aplicaciones móviles, con el paso de la edad debemos tener en cuenta que nuestros rasgos biométricos faciales cambian significativamente y también las condiciones del entorno.

La investigación se centra en analizar la vulnerabilidad de la protección de datos personales en Ecuador, específicamente en el ámbito del almacenamiento en la nube y la marcación biométrica en entidades públicas y privadas, el estudio cualitativo y descriptivo se basa en un análisis exhaustivo de fuentes legales, informes oficiales, normativas vigentes y literatura académica relevante.

> Según datos del Consejo de Protección de Datos Personales (CPDP), apenas un 35% de las empresas en Ecuador ha adaptado sus procesos a las normativas vigentes, mientras que más del 50% de los ciudadanos desconoce cómo sus datos son utilizados por instituciones públicas y privadas, realidad que abre la puerta a posibles abusos, como la comercialización de información personal sin consentimiento. (UTPL, 2025)

Se examina la aplicación de la protección de datos personales en empresas públicas que utilizan la biometría en sus procesos laborales, destacando la importancia de informar a los usuarios sobre los riesgos y garantías asociados a la recopilación y almacenamiento de sus datos biométricos, las empresas deben implementar planes de acción efectivos para comunicar su procedimiento de marcación y asegurar la protección de la información personal de los usuarios, garantizando la transparencia y la seguridad en el tratamiento de sus datos.

#### 2.1.1.1.3 Implementación biométrica en las relaciones laborales públicas

La implementación de tecnologías biométricas en el sector público mejora la eficiencia y seguridad en la gestión del personal. Sin embargo, plantea problemas en la protección de datos personales y derechos fundamentales, ya que los datos biométricos son sensibles, es

fundamental evaluar su uso para garantizar el respeto a la privacidad y la proporcionalidad. Además, el consentimiento de los empleados no es siempre libre, lo que requiere medidas adicionales de protección y un equilibrio entre beneficios operativos y derechos individuales.

> Para la implementación sistemas biométricos de identificación de personas, se debe realizar el estudio de factibilidad y su implementación en instituciones que no posean, a través de las direcciones de informática, a través de su personal, se encargará de la adecuación del ambiente físico y del hardware en analizar las diferentes tecnologías de control de acceso a utilizar, tareas como instalación de equipos y medidas de seguridad ambientales. (Palma, 2019).

La mayoría de los empleadores emplea datos biométricos, como huellas dactilares o reconocimiento facial, para registrar las horas de entrada y salida de sus trabajadores, a diferencia de las contraseñas, estos datos son únicos e inmutables, por lo que necesitan una protección especial que garantice tanto la disponibilidad como la integridad de la información personal. Por esta razón, no es recomendable ni adecuado utilizar estos datos sin las medidas de seguridad necesarias, ya que podría vulnerarse la ley de protección de datos personales y afectar los derechos de los ciudadanos, especialmente si no se asegura que esta información se use únicamente para los fines autorizados y no para perjudicar a la persona.

No abarca una incidencia o una aplicabilidad general menos aún tiene un carácter como norma que debe ser cumplida, si bien en una relación laboral que se forma en un inicio el empleado otorga su consentimiento al empleador para tener estos datos, el consentimiento en este caso no puede considerarse libre, “esto se debe a que la relación empleador-trabajador se caracteriza por una subordinación estructural, que puede dar lugar a un temor reverencial” (Bonilla, 2025), con la relación jurídica que se ha consolidado con el empleado y empleador hace referencia a un relación asimétrica, que se cuestiona en el principal análisis con la capacidad del trabajador de otorgar un consentimiento libre pero ello no quiere decir que todo consentimiento otorgado por un trabajador sea un consentimiento cuestionable.

Desarrollando una breve comparación de la aplicación de un consentimiento informado en Ecuador la tenemos en el área de salud, según ACESS-Agencia Nacional de Regulación, Control y Vigilancia, acontece que:

> En medicina, el consentimiento informado es el procedimiento médico formal, una exigencia ética, y un derecho reconocido por las legislaciones de todos los países, cuyo objetivo es aplicar el principio de autonomía del paciente, es decir, la obligación de respetar a los pacientes como individuos y hacer honor a sus preferencias en cuidados médicos. (ACESS, 2022)

Aborda el consentimiento informado en el ámbito médico este para que prevalezca la ética legal y comunicativa que se le debe reconocer a la autonomía de un paciente para la toma de sus decisiones, que previamente estén informadas con esta presentación en el proceso relacionadas a la salud del paciente. Se define que el consentimiento explica la finalidad y el modo en el cual se va a aplicar al momento de aceptarlo teniendo en cuenta parámetros con el modelo actual del paternalismo médico tradicional destacando un desarrollo hacia un modelo más participativo y concentrado en las decisiones del paciente. El consentimiento le da coherencia y permite que la persona a la que se le otorgue pueda tener en cuenta sus decisiones sin que otros exploten las mismas, recalcando que el consentimiento informado no solo es un requisito legal aplicable sino una exigencia ética en las decisiones. Para que una persona sea parte de este proceso, se presenta una transición del modelo en base al desarrollo de las decisiones que se deben tomar en el ámbito de la salud se pone en relieve la información asegurando la comprensión como base de la toma de decisiones por parte del paciente haciendo énfasis que la persona a que se le otorga el consentimiento informado debe estar en plenas facultades físicas y mentales lo cual remite a criterio de capacidad y competencia para poder consolidarlo.

A diferencia del requisito legal y ético que debería seguir las mismas autoridades que necesitan un registro único y sensible como forma de asistencia laboral, se debe tener en cuenta que en la ley de protección de datos personales hasta el momento no consta un modelo de consentimiento y no existe una descripción en el ámbito de marcación de datos biométricos como registro de asistencia a la empresa. Por lo que estos datos personales que se consideran sensibles deberían ser de conocimiento y competencia para las autoridades mucho más allá del marco legal planteándose como una forma de ética hacia la integridad general de una persona con sus datos personales.

#### 2.1.1.2 Mecanismos de protección

La protección de datos personales es esencial para garantizar la privacidad en un mundo digital, incluye mecanismos técnicos, organizativos y legales que permiten un tratamiento

responsable de la información, dada la amplia recolección de datos, es fundamental implementar estos mecanismos para generar confianza en los usuarios y cumplir normativas internacionales, evitando riesgos reputacionales y legales para las organizaciones.

> Que las medidas no son únicamente de tipo legal, no pueden limitarse a recabar de manera correcta el consentimiento o trabajar en la adaptación de los contratos tipo. Estas medidas podrían ser de índole administrativo, técnico, relacionado con los sistemas utilizados y servidores que almacenan estos datos, e inclusive, en el ámbito del manejo y capacitación de sus recursos humanos. (Ponce, 2025)

Se requiere un enfoque integral para la protección de datos personales que abarque diferentes áreas, incluyendo la administración, la tecnología, la seguridad y los recursos humanos, esto implica que las organizaciones deben considerar todas las posibles vulnerabilidades y debilidades en su sistema de protección de datos.

Las medidas administrativas pueden incluir implementación de políticas y procedimiento y procedimientos claros para el manejo de datos personales.

Las medidas técnicas se puede incluir la implementación de tecnologías de seguridad como cifrados, autenticación y autorización, así como la utilización de servidores y sistemas seguros para almacenar y procesar datos personales.

#### 2.1.1.2.1 Codificación y seudonimización obligatorias.

Con el desarrollo de mecanismos de recolección de datos en todo el mundo, se han implementado diferentes maneras de agilizar este proceso, que ayuda a recabar información en grandes cantidades, este mismo conlleva una serie de pasos que son fórmulas que requiere el sistema tecnológico para empezar con la recaudación de información.

La codificación estructura la información para simplificar su envío y manejo en formato digital, funcionando como un protocolo estándar que sincroniza los datos recopilados por dispositivos.

> La codificación de datos es la actividad que muestra una transformación de información en un formato legible por un computador para su acopio y tratamiento, debemos tener en cuenta que existen diferentes tipos de codificación de datos y se analizará los tipos que están inmersos a nivel de un dispositivo biométrico. (ESIC University, 2023)

La codificación de datos transforma la información en un formato manejable por computadoras, que es esencial para el almacenamiento y análisis. Existen diversas codificaciones, especialmente relevantes en dispositivos biométricos, que manejan datos complejos y sensibles como huellas dactilares y reconocimiento facial. La precisión y seguridad en este proceso son cruciales para mantener la integridad y privacidad de la información. Además, la codificación de datos no solo apoya el funcionamiento digital, sino que es fundamental para la seguridad y eficiencia en tecnologías avanzadas, resaltando la necesidad de adaptar procesos a las características específicas de cada sistema.

De acuerdo con ESIC University (2023) “la codificación binaria es la que se implementa en gran mayoría únicamente puede utilizar símbolos 0 y 1 para poder representar su base de información, este tipo de codificación lo podemos apreciar en computadoras”. A diferencia de la codificación de caracteres que necesitan estos símbolos para poder interpretar un texto, se interpreta mediante símbolos letras y textos que al momento de copiarlo le da un valor a cada carácter para que el procesador pueda reconocerlo y almacenarlo. por otro lado, la codificación de imagen, audio y video tienen el fin de poder simplificar archivos sin perder en lo menos posible su contenido su transformación de datos se componen por algoritmos matemáticos que hacen el archivo crudo se pueda procesar a uno de menos tamaño y fácil de transformarse al momento de ser compartidos o almacenados.

La seudonimización se orienta a la protección de datos personales como un mecanismo de defensa ante la manipulación, esta misma busca tener los datos que existen en el almacenamiento ocultas y con mecanismos de protección se debe seguir un proceso para que estas puedan estar protegidas por la sustitución de seudónimos como identificadores personales, la forma de aplicar un identificador se basa en caracteres personales que son únicos al momento de generar un perfil para guardar la información este mismo actúa como una clave de acceso única porque no es de manera escrita o se pueda editar mucho menos corregir.

Este vínculo conocido básicamente como seudonimización suele sustentarse dentro de una tabla de correspondencia con el propósito de una identificación de la persona o si el mismo es indispensable acceder con el identificador previamente almacenado en su perfil, la importancia de la seudonimización es tener la delicada actividad de mantener ocultos los datos de las personas que se crean un perfil mediante el sistema tecnológico, de modo que no se puedan asociar sus datos personales en cuestión esto hace que sea más complejo

vincular una información personal con otra diferente en diferentes tipos de tratamientos de datos personales.

La seudonimización es una medida de protección eficaz para poder tener vínculos de datos personales a buen recaudo, especialmente en ocasiones donde existen el conjunto de datos sensibles y están almacenados sin comprometer la identidad o información del individuo, de manera que no se permite reemplazar el seudónimo y el registro sea único haciendo hace un vínculo seguro haciendo así que se mitigue el acceso no autorizado hacia estos registros de datos en el almacenamiento correspondiente (European Union Agency For Cybersegurity, 2022).

La seudonimización proporciona una conexión confiable entre los datos y la persona a la que pertenecen, esto ayuda a proteger la confidencialidad y reduce los riesgos, al mismo tiempo que se conserva la capacidad de controlar y analizar la información, por lo tanto, es una herramienta valiosa para proteger la privacidad en situaciones donde hay datos sensibles.

#### 2.1.1.2.2 Protocolos de seguimiento para el acceso a los datos y su modificación.

Los protocolos de seguimiento son una herramienta de inspección hacia el historial de actividad de manipulación, esta crea planes de acción que previenen un acceso no autorizado dentro de una base de datos en conjunto la misma que defiende por diferentes filtros de seguridad vinculados al perfil del registro biométrico de una persona, siendo este un mecanismo de protección que se anhela reforzar con cada año por el método de protección de datos personas en las empresas.

La implementación de políticas de control para obtener acceso a la información privada contribuye a las diferentes entidades públicas y privadas que la información de identificación personal, datos únicos del individuo y otra información de carácter sensible y confidencial sea incorrectamente manipuladas teniendo accesos a estos datos.

El tratamiento para los datos y su modificación representa una clara responsabilidad crítica para las empresas que requieren de un registro para tener en cuenta la asistencia laboral de una persona especialmente en un entorno que se regula por normativas escritas por la Ley Orgánica de Protección de Datos Personales en Ecuador, porque su finalidad es garantizar la seguridad en caso de almacenamiento de cada uno de sus datos de manera que sean modificados o no por el autor del mismo perfil y no alguien externo con algún tipo de manipulación, exige principios claros y las empresas están sujetas actuar con legalidad,

transparencia y responsabilidad en la gestión que tienen como manipuladores directos de la información almacenada (Pesántez, 2023).

Desarrollando un análisis de lo que requiere tener presente un protocolo que agilite la forma de no corromper las barreras de seguridad entran como disposiciones más relevantes la condición de estar obligados atribuir un consentimiento informado explícito de titulares, así como políticas que incluyan guías de acción en casos de una infiltración de datos no autorizada o como reconocer aquellos, con esto la veracidad de la protección y seguimiento de la seguridad de protección dentro de una empresa recae en excelencia, mientras se desarrolle nuevas formas de registros para mantener seguros estos perfiles laborales, así mismo las auditorías internas periódicas son una práctica esencial para garantizar la confidencialidad y prevenir vulneraciones al sistema.

Dentro de la direccional de seguridad de la información que establezca el Estado deberá contemplar de manera legal e integral mecanismos para poder salvaguardar los datos personales frente a cualquier situación de riesgo de infiltración no autorizada que comprometa información delicada de un individuo, esto implica la implementación de medidas preventivas y correctivas orientadas a mitigar cualquier hecho de vulneración dentro del almacenamiento de esta información, así como su divulgación y destrucción ya sea accidental o con fines ilícitos, estas disposiciones son fundamentales para garantizar la integridad y confidencialidad de la disponibilidad que se le otorga a la información personal en todo momento.

**2.1.1.2.3 Estándares de seguridad según el EGSI (Esquema Gubernamental de Seguridad de la Información).**

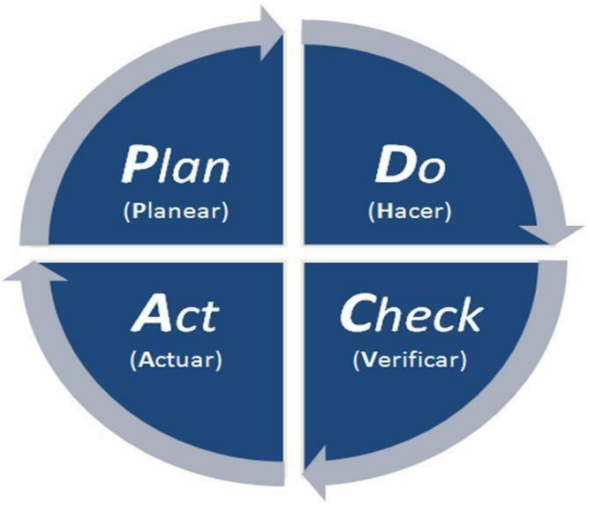
Se orienta a preservar los principios fundamentales de la confidencialidad, integridad y disponibilidad de la información manejada por las instituciones del sector público. Este objetivo alcanza mediante la adopción de un proceso estructurado de gestión de riesgos en materia de seguridad de la información, el que permite identificar, analizar y evaluar las amenazas potenciales, con bases en este análisis, se procede a la selección e implementación de controles específicos que permitan erradicar los riesgos identificados por el sistema fortaleciendo así la protección y el manejo adecuado de los activos de información personal.

El propósito de esquema gubernamental de seguridad de la información EGSI es preservar la confidencialidad de la información asumiendo una estructura de apoyo y planificación para la gestión de riesgos de seguridad de información el cual contempla la identificación personal y el tratamiento que tienen al momento de manipulación y alteración sobre los

principios que se están salvaguardando como objetivo de este esquema gubernamental, la seguridad de la información se alcanza mediante la aplicación de una serie de controles específicos estos que generan a través de un proceso adecuado de tratamiento una gestión de riesgos supervisados dentro del sistema de gestión de la seguridad de la información (Ministerio de Telecomunicaciones y de la Información, 2024).

Es aconsejable que los sistemas de gestión se desarrollen siguiendo un pleno enfoque que agilice su mejora constante, representado por el ciclo PDCA -Planificar, Hacer, Verificar y Actuar también conocido como ciclo Deming.

**Ilustración 1. Representación gráfica del ciclo Deming**




*Nota.* Información obtenida de (Betancourt, 2018).

El ciclo Deming es un enfoque sistemático que permite a las organizaciones planificar, ejecutar, verificar y actuar sobre sus procesos y sistema de manera continua, puede ser aplicado en la gestión de datos personales lo puede ayudar y garantizar la privacidad y la seguridad de los datos

### 2.1.2. Marcación pública como variable operativa

Dentro del desarrollo de un análisis de investigación lo que representa una variable operativa es una forma de contemplar e ilustrar un concepto abstracto el mismo que facilite un mecanismo de análisis dentro del estudio, “el proceso de definición de variables comienza desde que se define el problema de estudio y se formulan los objetivos, y es uno de los pasos más difíciles de la investigación” (Salusplay, 2025) a su vez se obtiene una definición dentro de la función en la investigación por lo cual complementa un supuesto de echo en materia manejable y manipulable a lo largo del desarrollo de las diferentes operaciones.

Dentro de la operación de investigación que será la variable como un núcleo y comienzo de una previa definición esta está ajustada al tipo de análisis que corresponde al estudio, esta conlleva a tener una dimensión la misma que descompone un tema en diferentes puntos de vista así mismo estudios previos incluso trabajos investigativos que complementen el estudio analizado estas diferentes dimensiones deben ser indicadores mismos que se deben medir al grado de aportación al desarrollo de la investigación de tal manera que este indicador pueda ser la medida de la dimensión y la dimensión sea la división de estudios de investigación que es nuestra variable operacional.

El análisis dentro de las definiciones que le damos a nuestras variables contempla mucho el fin del desarrollo de nuestra investigación, la misma que plantea diferentes teorías que ayudan a una argumentación de afirmación de nuestro proceso el mismo que puede presentar derivados de problemas que se puedan medir dentro del campo social.

De acuerdo con Monforte (2023) “los datos biométricos también pueden emplearse como método de control de acceso a las instalaciones de una empresa, institución o a cualquier área en la que se requiera gran seguridad y solo puedan acceder personas autorizadas”, la marcación pública entra como una variable de acceso visible esta es la acción de identificar mediante reconocimiento facial o huella dactilar el perfil de una persona en un grupo o una sociedad, en el marco conceptual la marcación biométrica actúa por un ente e almacenamiento de una institución con fines de reconocimiento de personas con perfiles selectos. La operación de esta variable se mide por reconocimientos de una presencia de la señal visible, la que indique automáticamente la trasformación de un individuo en el estatus determinado esto quiere decir que los medios de medición vienen de una lista almacenada una etiqueta incluso cuenta los objetos alrededor de la señal visible.

#### 2.1.2.1 Concepto y aplicación

La marcación con datos biométricos es una forma de almacenamiento de datos de una persona dentro de una corporación, la misma que identifica por reconocimiento facial o huellas dactilares datos sensibles de una persona de forma exclusiva, las características físicas de una persona son patrones que hacen un perfil dentro de la señal visible de la biometría para reconocer de forma inmediata el listado de datos del autor activo.

En el sector público esta manera de marcación en el ámbito laboral se ha implementado rápidamente en varias áreas para asegurar una eficiencia, seguridad y rapidez al momento

del cumplimiento del horario de ingreso y salida de los empleados, el uso primordial de esta marcación es el registro de cada perfil exclusivo asegurando la asistencia laboral teniendo así la ventaja de la justificación de la inasistencia, la misma que beneficia a la empresa en la proactividad de sus funciones de cada área.

> Según Arias,(2025) en su informe manifiesta que, debido a su creciente utilización en diversos ámbitos, especialmente en el entorno laboral, ha generado un intenso debate sobre la privacidad y los derechos de los individuos. En el ámbito laboral, la recopilación y procesamiento de datos biométricos ofrecen ventajas para las empresas en términos de seguridad y eficiencia ya que se utilizan para tener una herramienta de control dentro del establecimiento empresarial. Sin embargo, esta práctica plantea riesgos significativos para la privacidad y la autonomía de los trabajadores, especialmente en la relación laboral, donde los empleados suelen tener una posición más débil frente a sus empleadores, exacerba los riesgos asociados a la recopilación y almacenamiento de datos biométricos, teniendo potenciales consecuencias éticas y sociales importantes que deben ser atendidas.

Dentro de la protección de estos datos sensibles se debe prever de un manejo no autorizado en el ámbito laboral, porque la recopilación que se ha hecho anteriormente no cuenta con una previa autorización y esta misma es la que pone en riesgo la manipulación de estos datos que son considerados como datos sensibles.

#### 2.1.2.1.1 Finalidad de las marcaciones

En la actualidad diferentes formas de registro de marcación de acción han incrementado dentro los protocolos laborales con el fin de poder almacenar de forma rápida y diaria la acción del personal activo de la empresa, ha tomado gran relevancia esto debido a que nos otorga el derecho de exclusividad dentro de nuestro perfil en la marcación biométrica por la huella dactilar o reconocimiento facial del titular.

Debe considerarse que no todas las marcas cumplen con los requisitos para poder ser registradas, esto quiere decir que carecen de condiciones para que sean aceptadas y sostener lo contrario constituye un desacierto, para que una marcación esté registrada depende a gran medida que se pueda distinguir dándole una exclusividad al perfil, permite al usuario al mismo tiempo acceder a su perfil sin tener que implementar una nueva contraseña porque esta cuenta con una credencial única biométrica con ella puede mostrar los horarios laborales

activos a los que se ha ingresado, y salidas de instituciones poniendo alerta si existe algún retraso o no existe la marcación debida en el registro diario.

Una marcación cuenta como un registro único de nuestra actividad laboral, dentro de la empresa este es el fin, obtener un registro del horario de entrada y salida de su personal no obstante existe la inconsistencia de la información real y directa hacia el perfil creado para detectar su información y donde se almacena la misma (Software Público Ecuador, 2019).

La finalidad de una marcación se basa en la responsabilidad de asistencia, esta misma que en la actualidad no puede darse de forma presencial directamente con el jefe si no se usa la biometría para poder registrarte y como antes mencionado sirve para manejar grandes cantidades de personal, directamente se asimila como una forma muy ágil de poder hacer más eficiente el desarrollo de una entidad pública pero más allá de un registro se compromete los datos personales y de alguna forma se crea una subordinación de poder la misma que el Estado tienen en inobservancia, cuando nuestra constitución ampara el derecho a la protección de datos personales y la misma tiene como finalidad la garantía de la transparencia en la manipulación de estos datos.

#### 2.1.2.1.2 Riesgos identificados: exposición de datos y re-identificación

El riesgo de que los datos personales o sensibles sean accesibles a personas no autorizadas, debido a una falla de seguridad, error humano, ataque cibernético, o que los datos anonimizados, seudonimizados sean re-identificados, es decir que se pueda determinar la identidad de una persona a la que pertenecen los datos. Esto puede llevar a la pérdida o robo o divulgación no autorizada de datos.

Toda organización que anonimizan datos debe tomar medidas para garantizar que sus procesos son efectivos y que cumplan con la debida protección de datos sensibles.

Según informes la Agencia Española de Protección de Datos (2024) ha lanzado una nota técnica sobre la K-anonimidad, dirigida a organizaciones que anonimizan datos, el documento busca analizar la efectividad de la anonimización y reducir el riesgo de re-identificación, esencialmente para garantizar que los datos permanezcan verdaderamente anónimos.

Considerando el 26 del RGPD, establece que los datos personales seudonimizados permiten la identificación de personas físicas mediante factores y medios objetivos, considerando costes y tecnología (Agencia Española Protección datos, 2024).

En relación con la protección de datos personales es importante destacar que la anonimización y la seudonimización son estrategias fundaméntales para proteger la seguridad y privacidad de los datos sensibles, además reemplaza esta información con seudónimos o identificador único, mientras que la anonimización elimina o modifica la información personal identificativa.

Según Sieiro (2019) establece que la K-anonimidad es una propiedad esencial en la anonimia de datos, que mide la efectividad en la preservación de la identidad de los sujetos en conjuntos de datos donde se han eliminado identificadores. Esta métrica evalúa el riesgo de que terceros puedan acceder a información personal sensible, lo que es fundamental para garantizar la privacidad en la gestión de datos anonimizados.

Considero que la K-anonimidad puede ser una herramienta muy útil para proteger la privacidad de las personas, esta herramienta podría ser utilizada en diferentes áreas como salud o educación, lo que se busca es equilibrar la necesidad de proteger la privacidad y evitar la exposición de datos.

El proceso básico de anonimización consiste en disociar de los identificadores el resto de los datos más genéricos asociados a un sujeto como la fecha de nacimiento, el municipio de residencia, el género, etc. El conjunto de datos preservados serán aquellos necesarios para cumplir con el objetivo del tratamiento y, mediante la su conservación y enriquecimiento, explotarlo para extraer información adicional. (Agencia Española Protección datos, 2024)

**Ilustración 2. Anonimización**


*Nota.* Elaborado por los autores Luis Tircio y Leonel León, es la ilustración del proceso de anonimización.

Estas técnicas de anonimización y seudonimización permiten a las organizaciones proteger sus datos sensibles y reducir el riesgo de exposición y re-identificación. Sim embargo estas estrategias no son soluciones definitivas y requieren implementaciones cuidadosas y vigilancia constante para su efectividad.

Según Sieiro (2019) afirma que además de la metodología utilizada por aquellos que dirigen o controlan la información personal, es fundamental garantizar su privacidad, eliminar características identificativas podría no ser suficiente, ya que la combinación de datos de diferentes fuentes puede dar lugar a seudoidentificadores que comprometan la privacidad de las personas.

#### 2.1.2.1.3 Caso IESS 2024: suplantación mediante marcaciones inadecuadas

Considerando la importancia de la protección de datos sensibles en Ecuador, el Instituto Ecuatoriano de Seguridad Social (IESS) ha presentado vulnerabilidades en la protección de datos personales. En el año 2024 se han reportado incidentes relacionados con a la vulneración de datos sensibles, lo que generó preocupación sobre la efectividad de las medidas de seguridad implementadas. Este caso de estudio se basa en una búsqueda documental exhaustiva, que incluyen normativas legales, informes oficiales para analizar las causas y consecuencias de esta vulneración.

Según el diario La Hora (2024) afirma que, en noviembre del año 2024 un grupo de jubilados del Instituto Ecuatoriano de Seguridad Social (IESS) indicaron que sus pagos de pensiones llegaban con descuentos debido a préstamos que ellos nunca realizaron. Adicional denunciaron que sus contraseñas del IESS fueron cambiadas sin sus consentimientos. Lo que da a demostrar la complicidad interna de funcionarios del IESS. Los jubilados afectados señalan que este tipo de acciones no pueden realizarse sin el consentimiento o participación de empleados del IESS.

**Tabla 1. Vulneración y medidas adoptadas en el caso IESS**

| VULNERACIONES | MEDIDAS ADOPTADAS |
|---|---|
| Suplantación de identidad. | • Identificación IP.<br>• Identificación de empleados implicados.<br>• Revisión del sistema. |
| Descuentos indebidos. | • Ajustar los pagos, se siguen descontado los créditos a los jubilados perjudicados. |
| Información desactualizada | • Actualización en base datos.<br>• Acciones legales para proteger los derechos constitucionales. |

*Nota*. Elaborado por los autores Luis Tircio y Leonel León en base al Diario la Hora (2024).

La exposición indebida de datos personales o sensibles trae como consecuencias la suplantación de identidad, robo de información y pérdida de confianza en las instituciones. En el caso IESS la fata de seguridad dejo vulnerables a las personas y a la explotación de sus datos personales.

#### 2.1.2.2 Riesgos en su aplicación

En el desarrollo de la implementación de la biometría en el sector público se ha comprobado un crecimiento extenso, la misma que surge de la necesidad de recabar y regular la información de marcación de forma rápida optimizando la seguridad de datos en un almacenamiento o base de datos.

El uso de la huella dactilar y el reconocimiento facial dentro de la biometría crea una tendencia de inquietud dentro de la sociedad referente a la privacidad dentro de cada persona que es procesada en la marcación de estos datos, la seguridad de una base de datos en gran escala amerita una coordinación y organización fundamental, dado que uno de los derechos fundamentales es la seguridad de los datos sensibles el mismo que ampara la Constitución del Ecuador.

> La manipulación de este tipo de datos puede ser un acto de emergencia en la sociedad y un atentado ante la seguridad personal las filtraciones o la falta de regulación en su transformación es la necesidad que emerge dentro de este uso de marcación biométrica que necesita garantías que ayuden a la protección del perfil único de cada persona. (Bustamante Fabara, 2025)

La aplicación en el sector público contribuye a la eficiencia del registro, no obstante, conlleva varias alteraciones que ponen en riesgo su aplicación sin una verificación de autenticidad meticulosa para evitar vulneraciones al centro de almacenamiento de estos datos sensibles entrando en la necesidad de la responsabilidad ante la manipulación y el correcto uso de este historial de datos.

##### 2.1.2.2.1 Falta de actualización tecnológica en las instituciones públicas

En las instituciones públicas la actualización tecnológica se presenta como un obstáculo significativo para la eficiencia y la transparencia en gestiones públicas. A partir de esta realidad surge analizar las causas y consecuencias de esta falta de actualización.

Por lo que Godoy (2024) explica que “dentro de los datos personales existen unas categorías especiales, que ameritan un sistema reforzado de protección debido a que su uso se considera de alto riesgo. Estos datos son los denominados datos biométricos”.

En relación con lo que menciona Godoy (2024) la actualización tecnología, la implementación de sistemas reforzados son factores importantes para la protección de los datos biométricos en las instituciones públicas, lo que proporcionaría varios beneficios incluyendo:

- Mejoras de la seguridad.
- Incremento de confianza.
- Reducción de costos.

El acceso no autorizado a información confidencial el robo de identidad y suplantación pueden ser consecuencias por la falta de actualización tecnológica en las instituciones públicas. “Aunque los datos biométricos son difíciles de falsificar, los sistemas biométricos pueden ser vulnerables a ataques. Una vez que se produce una brecha de seguridad, es muy difícil recuperar el control sobre estos datos” (Godoy, 2024).

La falta de actualización de tecnología en las instituciones públicas requiere de una atención especial, es importante destacar la vulnerabilidad de los sistemas biométricos, y las consecuencias que puede tener la seguridad y la privacidad de los datos personales.

Según Unda (2024) establece que, el uso de datos biométricos tiene mayor riesgo de sufrir fallas de seguridad y violaciones de privacidad, lo que puede causar daños económicos y pérdidas importantes, es fundamental considerar opciones menos agresivas e implementar medidas de control para disminuir riesgos y proteger la privacidad y seguridad de las personas.

Es fundamental que las instituciones públicas inviertan en tecnologías de seguridad avanzadas y capacitación del personal para garantizar la privacidad y seguridad de las personas. A través de la actualización tecnológica se podrá asegurar la protección de datos sensibles.

#### 2.1.2.2.2 Incumplimiento de los protocolos de confidencialidad

La confidencialidad es un principio fundamental en la protección de datos sensibles, el incumplimiento de la confidencialidad es un gran problema en la actualidad, donde la

información sensible confidencial cada vez más se encuentra expuesta a riesgos de seguridad.

Es fundamental implementar técnicas y medidas organizativas para asegurar la confidencialidad de la información.

Como destaca Santander (2024) existen varias medidas que se pueden utilizar para proteger la información confidencial tales como:

- Cifrado de datos: proteger la información con claves y certificados para que solo las personas autorizadas puedan acceder a ellas.
- Controles de acceso: restringir el acceso a sistemas y redes donde se almacena y transmite la información.
- Clasificación de información: establecer procedimientos para clasificar y tratar la información según su valor y sensibilidad.
- Formación y concienciación: capacitar a las personas sobre la importancia de la confidencialidad y protección de la información.
- Acuerdos de confidencialidad: establecer acuerdos formales con los empleados que acceden a información confidencial para garantizar su protección.

Según Córdoba (2023) menciona que "la falta de regulaciones ha hecho que los países se vuelvan más propensos a la exposición de información confidencial."

Como señala Córdoba (2023), la falta de normas claras y efectivas ha hecho que las instituciones públicas de diferentes países se vuelvan más propensas a la exposición de información confidencial como, la filtración de datos personales o sensibles.

Ecuador en los últimos años ha tomado medidas importantes para proteger los derechos de privacidad y confidencialidad de los datos personales, una de las acciones más destacada fue la expedición del Reglamento de la Ley Orgánica de Protección de Datos Personales (RLOPDP), emitido por el ex presidente del Ecuador Guillermo Lasso el 6 de noviembre del año 2023 mediante Decreto Ejecutivo Nº 904. Este reglamento lo que busca es proteger los derechos de los titulares de los datos personales.

El Reglamento Ley Orgánica de Protección de Datos Personales consta de 14 capítulos, que regulan principalmente:

- Derechos de los titulares: acceso, rectificación, actualización, eliminación, oposición y portabilidad de datos.
- Autoridad de protección de datos: funcionamiento y registro publico
- Actores involucrados: regulaciones específicas para responsables delegados y encargados.
- Creación de superintendencia: supeditada a la disponibilidad presupuestaria y dictamen favorable del registro de finanzas (Reglamento a la Ley Orgánica de Protección de Datos Personales, 2023).

A partir de la implementación de la Ley Orgánica de Protección de Datos Personales (LOPD) del Ecuador es necesario analizar la efectividad en la protección de los derechos de privacidad y confidencialidad de los datos personales o sensibles. La anonimización se presenta para proteger la privacidad, pero su efectividad depende de la supervisión y del control adecuado.

#### 2.1.2.2.3 Delimitaciones en la formación del personal administrativo

La implementación efectiva en la marcación biométrica depende en gran medida de la capacidad que tiene el personal administrativo para utilizarlos y controlarlos adecuadamente, la falta de capacitación adecuada en el uso de datos biométricos puede generar riesgos, como violaciones a la privacidad o defectos en la identificación, la complejidad del uso de datos biométricos requiere el conocimiento especializado especialmente en el personal que los controla.

Mediante la formación y capacitación del personal administrativo, las instituciones en el sector público pueden mejorar considerablemente las prácticas en el uso de la biometría, garantizando eficiencia, seguridad y precisión en la identificación de las personas.

Por lo que Valle (2022) determina que “los organismos públicos deben implementar políticas y prácticas de privacidad que garanticen la recopilación y el almacenamiento seguros de información biométrica”.

La información biométrica es sensible y personal, y su mal uso o exposición puede tener consecuencias graves. Por lo tanto, es fundamental que las instituciones públicas mediante su personal debidamente capacitado tomen medidas para proteger esta información y garantizar la privacidad de las personas

Según Valle (2022) sugiere, diferentes estrategias efectivas de privacidad para la gestión de datos biométricos, que se almacenen versiones cifradas de datos biométricos en lugar de información sin procesar, como almacenar un patrón facial en lugar de imágenes directas, también se recomienda restringir los usos adicionales de estos datos, requiriendo consentimiento explícito y evitando aquellos que puedan resultar en perjuicio. Especialmente en el entorno de las fuerzas del orden o las autoridades de migración, es fundamental limitar el acceso interno a datos biométricos solo al personal esencial y adoptar un método de reducción de datos, asegurando que solo se recolecten los datos indispensables y se eliminen cuando ya no sean necesarios, estas medidas son fundamentales para proteger la privacidad de los usuarios y evitar violaciones de datos.

La adopción de medidas como el almacenamiento de versiones cifradas, limitación de usos secundarios, restricción del acceso interno y la minimización de datos son esenciales para prevenir filtraciones de datos y garantizar la protección de información sensible.

### 2.1.3 Efectividad de protección en las instituciones públicas

La protección de la información dentro de las instituciones públicas se convierte en una prioridad fundamental para la sociedad y el personal superior a cargo de la inspección de la seguridad de este almacenamiento interno, “la pérdida de estos datos podría tener consecuencias desastrosas para las empresas o los particulares, por lo que la protección de datos es ciertamente necesaria” (Buenning, 2025). Dentro de las diferentes formas de manipulación y amenazas que presentan este tipo de datos cibernéticos tenemos también la implementación de efectividad dentro de un plan de seguridad que son diferentes formas de organización ya contempladas que ayudan a fundamentar la investigación.

El uso de huellas dactilares contempla un patrón de escaneo consecutivo el mismo que crea un perfil y da uso a la marcación de un horario dentro de un sistema laboral, al igual que el reconocimiento facial según Uguina (2024) “es una tecnología probabilística que puede reconocer automáticamente a las personas por su rostro para autenticarlas o identificarlas” (p. 13), no obstante, este proceso depende de múltiples factores para garantizar su efectividad tanto la calidad de la tecnología biométrica y el dispositivo de marcación.

Analizar y garantizar la efectividad de la protección de datos dentro de la institución pública no se basa en la organización ante situaciones de emergencia, sino también en el apoyo

público que exista para la garantía de responsabilidad de una autoridad suprema, esta que fundamente una transparencia y agilice la confianza en la institución.

#### 2.1.3.1 Indicadores de medición

Dentro de las diferentes formas que sustentan una efectividad de seguridad de los datos personales mediante la marcación biométrica, el aumento de factores que fortalezcan la protección juega un papel fundamental en cada sector público que ha implementado esta tecnología.

Los indicadores de medición valoran la efectividad del proceso de tratamiento, estos datos pueden aislarse, contraerse o enfrentarse. El tratamiento de los datos personales hace posible un historial táctico de una persona al permitir el registro de una serie de datos que crean un perfil autentico de una persona que separadamente carecen de importancia. La obtención de un perfil supone establecer una correlación entre la posesión que tiene una persona por sus características y comportamiento concretos dentro de la sociedad en función del resultado dado al marcar en biometría sus datos (Garrija, 2004).

La implementación de la biometría debe realizarse bajo indicadores que permitan analizarse de manera objetiva en el sector público, debido a si amplitud de sistemas el reducirlo ayudara a su adecuada aplicación dentro de la toma de decisiones para mejorar la seguridad empresarial y laboral y que esta vaya sujeta al derecho fundamental de los ciudadanos.

En consecuencia, su uso debe ser responsable, así como su tratamiento de manipulación la misma que se obtendrá a través de los diferentes sistemas de organización ante diferentes emergencias y que estas protejan la actividad del registro a un perfil.

##### 2.1.3.1.1 Índice de incidentes por filtración (caso reportado en el año 2024)

Las instituciones públicas deben tomar medidas efectivas para proteger la información biométrica, y prevenir incidente de seguridad como la filtración de datos sensibles.

“La tasa de filtraciones y pérdidas de datos refleja la seguridad y precisión, reduciendo riesgos empresariales vinculados al manejo incorrecto de información” (Secureframe, 2025).

Un ejemplo reciente de la importancia que tiene la seguridad de la información de datos es el caso reportado en el 2024, donde se sufrió filtraciones de datos biométricos que afecto a muchas personas.

Según informes de diario el Expreso (2024) indico la siguiente noticia:

> En 2024, se han registrado más de 1.500 millones de registros expuestos debido a filtraciones de datos en numerosas grandes empresas. Las vulnerabilidades en la seguridad, particularmente la falta de autenticación multifactor, han facilitado los ciberataques. Un caso destacado fue el ataque a UnitedHealth, que afectó a un tercio de la población estadounidense por la falta de medidas adecuadas de seguridad en Change Healthcare. Otros ejemplos incluyen incidentes en TicketMaster y AT&T, comprometiendo datos de cientos de millones de usuarios.

Este caso destaca la necesidad de que las instituciones públicas deben implementar medidas efectivas para proteger los datos sensibles y prevenir incidente de filtración.

Según Espinoza (2024) mediante diario el Expreso afirma que, ESET alerta que los ataques cibernéticos se aprovechan de políticas de seguridad inadecuadas y credenciales mal gestionadas. La educación en seguridad y tecnologías robustas son clave para disminuir el riesgo de filtraciones.

Las instituciones públicas deben priorizar la seguridad cibernética, la educación y la conciencia sobre la seguridad cibernética son fundamentales para prevenir ataques cibernéticos, esta requiere implementación de medidas de seguridad efectivas para garantizar que no se filtre información o datos sensibles.

#### 2.1.3.2 Factores condicionantes

##### 2.1.3.1.2 Diferencias tecnológicas entre instituciones

La adopción del uso de la biometría en el sector público no es uniforme en todas las instituciones, lo que puede generar diferencias en la forma en la que se recopilan, almacenan y procesan los datos biométricos.

Uno de los factores principales que origina diferencia tecnológica entre instituciones del sector público en el uso de datos biométricos es:

- Inversión en tecnología: algunas instituciones públicas tienen más recursos para invertir en tecnología biométrica, mientras otras instituciones tienen limitaciones presupuestarias.

Según Aratek (2023) establece que, existen varias modalidades de sistemas biométricos:

- La biometría física que se refiere a métodos como el reconocimiento facial, geometría de mano, reconocimiento de huellas dactilares y escáner de iris.
- La biometría conductual que se enfoca en aspectos conductuales como la dinámica de pulsación de teclas, el reconocimiento de voz, y el análisis de la marcha.

Las instituciones públicas pueden escoger diferentes tecnologías biométricas de acuerdo con sus objetivos y necesidades, lo que puede generar diferencias en la forma que se gestionan o se implementan los datos biométricos. Las diversas modalidades de sistemas biométricos pueden generar retos de interoperabilidad, lo que puede afectar la eficacia en la gestión de datos biométricos, esto puede generar diferencias entre instituciones en la forma de cómo se almacenan, recopilan y procesan los datos sensibles.

**Tabla 2: Ejemplo ilustrativo de diferencias tecnológicas en instituciones públicas.**

| INSTITUCIÓN | TECNOLOGÍA BIOMÉTRICA | INTEROPERABILIDAD | NIVEL DE SEGURIDAD | COSTO DE IMPLEMENTACIÓN |
|---|---|---|---|---|
| Upse | Código Qr | Alta | Alta | Alta |
| Municipio de Santa Elena | Huella Dactilar | Alta | Media | Media |
| Municipio de Salinas | Reconocimiento Facial | Alta | Bajo | Media |
| Municipio de la Libertad | Huella Dactilar | Media | Bajo | Bajo |

*Nota*. Modelo comparativo (diferenciación de tecnologías biométricas en las instituciones) elaborado por autores Luis Tircio y Leonel León.

Es importante considerar cuidadosamente las implicaciones de cada tecnología antes de implementadas en las instituciones públicas, cada tecnología tiene sus propias ventajas y desventajas.

#### 2.1.3.2.2 Conflictos de transparencia administrativa y protección de datos

La importancia sobre el equilibrio entre la transparencia administrativa y la protección de datos ha sido un factor fundamental para garantizar la rendición de cuenta y confianza en las instituciones públicas. Al mismo tiempo la transparencia administrativa requiere que las instituciones públicas sean abiertas y transparentes en toma de decisiones y funcionamiento, lo que permite a los ciudadanos acceder a información sobre la forma en cómo se utilizan los recursos del estado.

La protección de datos requiere que las instituciones públicas implementen medidas efectivas de seguridad, para proteger los datos sensibles y garantizar que se utilicen de manera legitima y transparente.

El equilibrio adecuado entre transparencia y privacidad requiere acceso limitado a la información y medidas de seguridad sólidas, además es fundamental tener en cuenta los factores contextuales y respetar los derechos de privacidad al diseñar e implementar políticas de transparencia (Castro, 2024).

Las políticas de transparencia deben ser estructuradas e implementadas de manera que equilibren la necesidad del acceso a la información con la protección de la información personal o sensible. Consecutivamente deben respetar los derechos de privacidad de las personas y de las instituciones públicas, el acceso de la información debe ser estrictamente controlado y restringido según sea necesario.

> Según Castro (2024) para lograr el equilibrio entre la transparencia y la seguridad de los datos en el sector público es un desafío complejo, que requiere un enfoque cuidadoso y considerado. Las decisiones deben basarse en un análisis detallado de los riesgos y beneficios, y deben involucrar a todas las partes interesadas, para garantizar que se protejan tanto la privacidad de los individuos como el interés público.

**Ilustración 3. Equilibrio entre transparencia administrativa y la protección de datos**

*Nota*. Ilustración del equilibrio entre transparencia y privacidad, elaborado por los autores Luis Tircio y Leonel

Lograr el equilibrio entre la transparencia y la protección de los datos es muy complejo, debido a que la transparencia administrativa requiere la divulgación de la información, por otro lado, la protección de datos tiene como misión principal salvaguardarla, esto implicaría que es necesario evaluar los posibles riesgos de divulgación de información sensible, así como los beneficios de transparencia.

## 2.2 MARCO LEGAL

### 2.2.1 Constitución de la República del Ecuador

#### 2.2.1.1 Principios generales sobre el ejercicio de derechos

En el artículo 11, numeral 2, de la Constitución (2008) menciona lo siguiente:

> Todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades. Nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos. La ley sancionará toda forma de discriminación. El Estado adoptará medidas de acción afirmativa que promuevan la igualdad real en favor de los titulares de derechos que se encuentren en situación de desigualdad. (Constitución de la Republica del Ecuador, 2008)

Todas las personas deben ser tratadas de manera igualitaria ante la ley, sin discriminación por razones de etnia, género, edad, orientación sexual, discapacidad, entre otras. El Estado debe proteger a las personas contra cualquier forma de discriminación, así mismo garantizar la igualdad y no discriminación en la sociedad, lo que es fundamental para promover la justicia y la dignidad de todas las personas.

#### 2.2.1.2 Desarrollo progresivo de los derechos

En el artículo 11, numeral 8, de la Constitución menciona lo siguiente:

"El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio" (Constitución de la Republica del Ecuador, 2008).

El Estado tiene la responsabilidad de generar y garantizar las condiciones necesarias para el pleno reconocimiento y ejercicio de los derechos, lo que implica:

- Progresividad: el Estado debe trabajar para ampliar y profundizar los derechos de manera continua.
- Garantía: el Estado debe asegurar que se cumplan las condiciones necesarias para el ejercicio efectivo de los derechos.

#### 2.2.1.3 Derecho a la protección de datos personales

En el artículo 66, numeral 19, de la Constitución menciona lo siguiente

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008)

Toda persona tiene derecho a acceder y decidir sobre la información y datos personales que se recopilan, almacenan y procesan y el Estado está en la obligación de proteger la privacidad de los individuos y garantizar que sus datos personales no sean utilizados de manera indebida.

### 2.2.2 Ley Orgánica de Protección de Datos (LOPDP)

#### 2.2.2.1 Objeto y finalidad

La Ley Orgánica de Protección de Datos en el artículo 1 establece lo siguiente:

> El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (Ley Orgánica de Protección de Datos Personales, 2021)

La ley busca proteger el derecho de las personas a controlar sus datos personales y garantizar su privacidad, regula los principios, derechos y obligaciones relacionados con la protección de datos personales y también establece mecanismos para proteger y hacer cumplir los derechos y obligaciones relacionados con la protección de datos personales.

#### 2.2.2.2 Términos y definiciones

La Ley Orgánica de Protección de Datos en el artículo 4 establece lo siguiente:

“Base de datos o fichero: conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica” (Ley Orgánica de Protección de Datos, 2021)

Un conjunto organizado de datos que pueden ser de diferentes tipos y formas también incluye diferentes tipos de almacenamiento y acceso como el centralizado, descentralizado o repartido de forma funcional o geográfica. Es importante establecer el alcance de la ley en cuanto a la protección de datos personales y determinar qué tipo de conjuntos de datos están sujetos a sus disposiciones.

Ley Orgánica de Protección de Datos en el artículo 4 menciona que el dato biométrico es un “Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros” (Ley Orgánica de Protección de Datos, 2021)**.**

Dato personal único se refiere a características que identifican de manera única a una persona, las características físicas o fisiológicas incluye rasgos como imágenes faciales, huellas dactilares, etc. Las conductas pueden incluir patrones de comportamiento que permitan la identificación, y la identificación única es el dato biométrico permite confirmar la identidad de una persona de manera precisa.

> Datos sensibles: relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. (Ley Orgánica de Protección de Datos, 2021)

Ciertos tipos de datos requieren una protección especial debido a su naturaleza sensible y el potencial riesgo de discriminación o daño si se manejan de manera inapropiada.

> Elaboración de perfiles: todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, Habilidad, ubicación, movimiento físico de una persona, entre otros. (Ley Orgánica de Protección de Datos, 2021)

Es de importancia considerar las implicaciones éticas y legales del uso de datos personales para crear perfiles, ya que puede afectar la privacidad y los derechos de las personas.

#### 2.2.2.3 Acceso a datos personales por parte del encargado

Ley Orgánica de Protección de Datos en el artículo 34 señala lo siguiente:

> No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones será considerado encargado del tratamiento. El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas, una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales, el encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley. (Ley Orgánica de Protección de Datos Personales, 2021)

El tratamiento de datos personales debe estar controlado por un contrato que establezca claramente las instrucciones del responsable y las obligaciones del encargado, donde el encargado solo puede tratar los datos de acuerdo a las instrucciones del responsable y no puede utilizarlos para finalidades diferentes, una vez cumplida la prestación contractual, los datos personales deben ser destruidos o devueltos al responsable del tratamiento y el encargado será el responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales, la finalidad es garantizar que los encargados del tratamiento de datos personales actúen de manera responsable y segura, y que se protejan los derechos de los titulares de los datos.

#### 2.2.2.4 Notificación de vulneración de seguridad

En el artículo 43 de la Ley Orgánica de Protección de Datos establece lo siguiente:

> Notificación de vulneración de seguridad.-El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación. El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella. (Ley Orgánica de Protección de Datos, 2021)

El responsable del tratamiento debe notificar a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones en un plazo de 5 días después de tener constancia de la vulneración, si es improbable que la vulneración constituya un riesgo para los derechos y libertades de las personas físicas, no se requiere notificación. Si la notificación se realiza después del plazo de 5 días, debe estar acompañada de una justificación de la dilación y el encargado del tratamiento debe notificar al responsable cualquier vulneración de seguridad de datos personales en un plazo de 2 días después de tener conocimiento de ella, con la finalidad de buscar garantizar que se tomen medidas rápidas y efectivas en caso de vulneraciones de seguridad de datos personales, y que se protejan los derechos de los titulares de los datos.

### 2.2.3 Política de Protección de Datos del Gobierno Autónomo Descentralizado de la Provincia de Santa Elena

#### 2.2.3.1 Términos y condiciones de uso de canales electrónicos

Según Administrador (2023) menciona, que los GAD de la provincia de santa elena establecen políticas de protección de datos personales como:

> Generalidades:
>
> El ingreso y uso de los canales electrónicos que el Gobierno Autónomo Descentralizado Provincial de Santa Elena dispone para brindar servicios a los

ciudadanos, le atribuye la condición de usuario; y la aceptación expresa, plena y sin reservas por parte del usuario, de todos y cada uno de los términos y condiciones de uso de la presente política, en la versión publicada.

El usuario tendrá acceso a la información publicada en la página web del Gobierno Autónomo Descentralizado Provincial de Santa Elena, sin embargo, para acceder a los servicios que requieren autenticación es necesario ingresar la identificación y clave de acceso.

El Gobierno Autónomo Descentralizado Provincial de Santa Elena brinda la seguridad de la información al usuario desde el momento en que se solicita la información personal, con la cual se puede identificar al usuario, asegurando que sólo se empleará de acuerdo con los términos y condiciones de uso de la presente política.

El GADPSE dispone de una página web institucional para presentar información a los ciudadanos sobre la gestión que realiza (Administrador, 2023).

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

Los Gobierno Autónomo Descentralizado serán responsable del tratamiento y uso de los datos personales recabados directamente a través de sus canales electrónicos, lo que garantiza la seguridad de la información personal y asegura que solo se empleará de acuerdo con los términos y condiciones, con el fin de proteger la privacidad y seguridad de los datos personales de los usuarios.

#### 2.2.3.2 Responsabilidad

El Gobierno Autónomo Descentralizado Provincial de Santa Elena se hará responsable de:

- Del tratamiento y uso de los datos personales que recabe en forma directa a través de sus canales electrónicos.
- Se deslinda de cualquier responsabilidad que pueda generar al usuario por cualquier uso inadecuado o contrario a los fines de sus canales electrónicos.
- No se hace responsable por la veracidad o exactitud de la información contenida en los enlaces a otros sitios web o que haya sido entregada por terceros.

El Gobierno Autónomo Descentralizado Provincial de Santa Elena no se responsabiliza de ningún daño o perjuicio sufrido por el usuario que se derive de la no disponibilidad de acceso a los canales electrónicos.

### 2.2.4 Tratados internacionales

#### 2.2.4.1 Convenio modernizado para la protección de las personas con respecto al tratamiento de datos personales-128 (2018)

Artículo 4 – Deberes de las partes:

> 1. Cada parte adoptará las medidas necesarias en su legislación para dar efecto a las disposiciones de la presente convención y asegurar su aplicación.
>
> 2. Estas medidas serán adoptadas por cada parte y deberán entrar en vigor en el momento de la ratificación o de la adhesión a la presente convención.

Cada parte se compromete a:

> a. Permitir que el Comité de la Convención previsto en el capítulo VI evalúe la eficacia de las medidas que haya adoptado en su legislación para dar efecto a las disposiciones de la presente convención; y
>
> b. Contribuir activamente a este proceso de evaluación. (COE Search - CM, 2018)

Cada parte debe adoptar medidas necesarias en su legislación para dar efecto a las disposiciones de la convención, esto implica que los gobiernos deben implementar medidas de seguridad adecuadas para la protección de los datos personales de los servidores públicos. Los gobiernos deben estar dispuestos a someterse a una evaluación externa por parte del comité de la convención, para garantizar que sus medidas de seguridad sean efectivas en la protección de datos biométricos.

**Artículo 6 – Categorías especiales de datos**

El tratamiento de:

- Datos genéticos.
- Datos personales relativos a delitos, procedimientos penales y condenas, y las medidas de seguridad relacionadas.
- Datos biométricos que identifican de forma única a una persona.

- Datos personales por la información que revelen relativa al origen racial o étnico, opiniones políticas, afiliación sindical, creencias religiosas o de otra índole, salud o vida sexual.

Sólo se permitirá cuando la ley contemple garantías adecuadas que complementen las de la presente la convención.

- Dichas garantías protegerán contra los riesgos que el tratamiento de datos sensibles pueda presentar para los intereses, derechos y libertades fundamentales del interesado, en particular el riesgo de discriminación. (COE Search - CM, 2018)

El tratamiento de datos biométricos solo se permitirá cuando la ley contemple garantías adecuadas que contemplen las de la convención, esto implica que los gobiernos deben establecer garantías específicas para proteger los derechos y libertades fundamentales de los ciudadanos.

**Artículo 9 – Derechos del interesado**

Toda persona tendrá derecho a:

a) No ser objeto de una decisión que le afecte significativamente basada únicamente en un tratamiento automatizado de datos sin que se haya tenido en cuenta su opinión.
b) Obtener, previa solicitud, a intervalos razonables y sin demora ni gastos excesivos, la confirmación de que se están tratando datos personales que le conciernen, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el plazo de conservación, así como cualquier otra información que el responsable esté obligado a proporcionar para garantizar la transparencia del tratamiento de conformidad con el artículo 8, apartado 1;
c) Para obtener, previa solicitud, conocimiento del razonamiento en el que se basa el tratamiento de datos cuando se le apliquen los resultados de dicho tratamiento.
d) Oponerse en cualquier momento, por motivos relacionados con su situación, al tratamiento de datos personales que le conciernan, salvo que el responsable acredite motivos legítimos para el tratamiento que prevalezcan sobre sus intereses o derechos y libertades fundamentales.
e) A obtener, previa solicitud, gratuitamente y sin demora excesiva, la rectificación o supresión, según el caso, de dichos datos si están siendo o han sido tratados en contravención de las disposiciones de la presente convención.

f) A tener un recurso conforme al artículo 12 cuando se hayan violado sus derechos conforme a esta convención.
g) A beneficiarse, sea cual sea su nacionalidad o residencia, de la asistencia de una autoridad de control en el sentido del artículo 15, en el ejercicio de sus derechos en virtud del presente Convenio.
h) El apartado “a” no se aplicará si la decisión está autorizada por una ley a la que esté sujeto el responsable del tratamiento y que establezca además medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos del interesado. (COE Search - CM, 2018)

Los interesados tienen derecho a obtener información sobre el tratamiento de sus datos personales, incluyendo el origen de sus datos el plazo de conservación y cualquier otra información relevante, es decir que los ciudadanos deben tener acceso a información clara y transparente sobre cómo se están utilizando sus datos biométricos, cada ciudadano debe tener la oportunidad de oponerse al uso de sus datos biométricos si consideran que no es necesario o que puede afectar sus derechos y libertades fundamentales, los interesados tienen derecho a obtener la corrección o eliminación de sus datos personales si están siendo tratados de manera incorrecta o en contravención de las disposiciones de la convención.

## 2.3 MARCO CONCEPTUAL

### Datos biométricos personales

Los datos biométricos siempre pueden considerarse como:

> Información sobre una persona física, ya que afectan a datos que proporcionan, por su propia naturaleza, información sobre una persona determinada. En el contexto de la identificación biométrica, la persona es generalmente identificable porque los datos biométricos se usan para identificar o autenticar/comprobar al menos en la medida en que el interesado se distingue de cualquier otro. (F. de Marcos, 2022, p. 220)

### Anonimización

"Se refiere a la aplicación de determinadas técnicas o procedimientos tendientes a impedir la identificación o reidentificación de una persona física sin que para ello sea necesario el empleo de esfuerzos desproporcionados." (F. de Marcos, 2022, p. 70)

### Consentimiento expreso

> La manifestación de la voluntad del titular mediante la cual acepta que sus datos personales sean tratados por el responsable en términos del aviso de privacidad que le fue puesto a su disposición. El consentimiento expreso, por su parte, requiere ser patente, especificado, lo que significa que requiere de una acción afirmativa por parte del titular. (F. de Marcos, 2022, p. 181)

### Seudonimización

> Es un procedimiento que, como medida de seguridad, se aplica al dato personal para reducir los riesgos derivados de su tratamiento, mediante la sustitución de un atributo en un registro (por lo general, un atributo único) por otro, de forma tal que se puedan Re identificar los datos mediante el empleo de información adicional y separada que permita volver a asignar el atributo correcto a cada registro. (F. de Marcos, 2022, p. 796)

**Suplantación de identidad**

> Es aquella actividad por la que una persona se hace pasar por otra usando, habitualmente, medios informáticos. Este fenómeno se produce asiduamente en la actualidad, debido al aumento exponencial de la comunicación y uso de medios telemáticos. Asimismo, la mayoría de las actividades económicas llevadas a cabo por las empresas en el presente, requieren del uso de nuevas tecnologías de la información, las cuales se encuentran expuestas a multitud de ciber amenazas en el ámbito de la seguridad de la información, entre las que cabe destacar la suplantación de identidad. (AUTELSI , 2021, p. 2)

**K-anonimidad**

"Es un método diseñado para evitar ataques en los que la combinación de distintos conjuntos de datos puede permitir el reconocimiento de individuos, incluso después de haber eliminado las propiedades que los identificaban directamente" (Martínez González, 2021, pág. 22).

**Interoperabilidad**

> Es la habilidad que poseen diversos sistemas para compartir e intercambiar información de forma eficiente, coherente y segura. En otros términos, significa que diversas plataformas puedan comunicarse entre sí y comprender los datos que reciben, sin perder su sentido ni exactitud. (Lezcano, 2023, p. 260)

**Taxativa**

> Este principio instaura que las normas deben expresar sus aparentes de hecho de manera concreta y precisa, evitando ambigüedad que pueden crear interpretaciones arbitrarias. Su propósito es asegurar que los individuos estén al tanto con claridad las conductas que la ley sanciona o en defecto regulan, fortaleciendo así la seguridad jurídica y el respeto a los derechos primordiales dentro del marco de lo legal. ( Silva Gallinato, 2018, p. 4)

# CAPÍTULO III

# MARCO METODOLÓGICO

## 3.1 Diseño y tipo de investigación

### 3.1.1 Diseño de investigación

El diseño de investigación es un plan sistemático y estructurado que guía la recopilación y el análisis de datos, con el fin de responder a las preguntas de investigación y alcanzar los objetivos del estudio.

Corona señala que:

> La investigación cualitativa es un paradigma emergente que sustenta su visión epistemológica y metodológica en las experiencias subjetivas e intersubjetivas de los sujetos, cuya práctica se orienta hacia la sociedad construida por el hombre, donde interactúan las versiones y opiniones del ser pensante, respecto a los hechos y fenómenos de estudio, para construir la realidad de manera cooperativa y dinámica. (Corona, 2018)

La presente investigación se enmarca en un enfoque cualitativo, que busca comprender y analizar, implicaciones legales, éticas y sociales desde la perspectiva de los actores involucrados en la implementación de sistemas de marcación con datos biométricos en el sector público de la provincia de Santa Elena. El enfoque cualitativo permite explorar, percepciones, experiencias y prácticas relacionadas con la protección de datos personales en las instituciones del sector público en el ámbito laboral.

### 3.1.2 Tipo de investigación

Es de tipo descriptiva y exploratoria. Es descriptiva porque busca identificar características, procedimientos y normativas actualizadas y vinculadas al uso de datos biométricos en la marcación laboral del sector público. Es exploratoria porque aborda un suceso poco estudiado en el entorno local, permitiendo identificar problemáticas, deficiencias normativas en la protección de datos personales

La investigación contribuirá a comprender mejor las implicaciones del uso de datos biométricos en la marcación laboral y su efecto en la protección de datos personales. Los resultados de la investigación podrán ser utilizados para informar políticas y prácticas relacionadas con la protección de datos personales del sector público.

## 3.2 Población

### 3.2.1 Población

La población está constituida por funcionarios y empleados de los GAD Municipales de Santa Elena, La Libertad, Salinas, y de la Universidad Estatal Península de Santa Elena (UPSE) de la provincia de Santa Elena, específicamente aquellos que trabajan en áreas relacionadas con la implementación y gestión del sistema de marcación biométrica, en nuestro estudio se consideró que nuestra población es finita relativamente pequeña para ser estudiada en su totalidad, lo que elimina la necesidad de seleccionar una muestra representativa, es decir que se trabajó bajo la figura de población absoluta.

**Tabla 3. Población**

| DESCRIPCIÓN | POBLACIÓN |
|---|---|
| Talento humano | 4 |
| Departamento de Tecnología de la Información y la Comunicación | 4 |
| Total | 8 |

*Nota*. Elaborado por los autores Luis Tircio y Leonel León.

## 3.3 Métodos, técnicas e instrumentos

### 3.3.1 Técnicas e Instrumentos

Entrevistas abiertas: Dirigidas a funcionarios públicos, técnicos y representantes de trabajadores, para indagar sobre sus percepciones, experiencias y conocimientos respecto a la protección de datos biométricos.

**Tabla 4. Métodos, técnicas e instrumentos**

| MÉTODO | TÉCNICA | INSTRUMENTO |
|---|---|---|
| Análisis documental. | Revisión documental. | Citas bibliográficas y análisis de normativas. |
| Interpretación fenomenológica. | Entrevista abierta. | Guía de entrevista para autoridades, técnicos y usuarios. |

| | | |
|---|---|---|
| Estudio de caso. | Análisis de incidentes y prácticas. | Registro de casos y estudio documental. |
| Encuesta descriptiva. | Aplicación de encuestas. | Cuestionarios para recolectar datos cuantitativos. |

*Nota*. Elaborado por los autores Luis Tircio y Leonel León.

Las técnicas utilizadas en el desarrollo de esta investigación dirigida hacia los 3 GAD municipales de la península de Santa Elena incluyendo a la UPSE específicamente a las autoridades de los departamentos de talento humano y sistemas fueron construidas como preguntas abiertas, detallando en nuestra planificación que una entrevista está compuesta con 6 preguntas dirigidas hacia el departamento de talento humano y una entrevista estructurada de 5 preguntas dirigidas hacia el departamento de sistemas y comunicaciones. La finalidad que tienen las preguntas que planteamos es que estos, nos brinden información original de sus métodos, protocolos y conocimiento dentro del área biométrica y sus respectivas formalidades para su uso, al ser instituciones públicas de la provincia de Santa Elena se manejan con diferentes tipos de tratamiento de la información biométrica y su conocimiento en la aplicación laboral es importante para determinar nuestra respuesta al estudio.

Es importante mencionar que el estudio hacia los tres GAD Municipales de la Península de Santa Elena y a la Universidad Estatal Península de Santa Elena se realizaron en base a la similitud de marcación biométrica de asistencia, siendo estas instituciones públicas que encajan perfectamente en nuestro estudio.

Se logró acceder a las instituciones para formular las entrevistas a los funcionarios de estos departamentos de forma presencial, acudiendo amablemente hacia su delegación donde de manera formal extendimos nuestro saludo y procedimos a identificarnos para poder tener su autorización, cabe recalcar que primero acudimos a UPSE por la cercanía, nos atendieron amablemente el área de Tics y de manera óptima realizamos las preguntas al encargado del área, para poder tener acceso a una entrevista con el área de talento humano tuvimos que agendar una cita, la misma que ayudo a concretar un día y hora directa en disponibilidad de la directora de talento humano.

Procedimos acudir presencialmente y solicitar una entrevista al GAD de Salinas donde amablemente nos la autorizaron en los dos departamentos, talento humano y sistemas fueron muy amables y respondieron todas nuestras preguntas que teníamos documentadas y listas para exponérselas, junto a esto el GAD de La libertad también nos brindó la disposición de autorizarnos la entrevista hacia los dos departamentos sin ningún percance adicional, grabamos las respuestas en audio y estas las guardamos en un chat apartado de nuestro dispositivo adicional fotografiamos como evidencias que serán anexadas al final de este documento.

Por ultimo acudimos al GAD de Santa Elena en el que tuvimos algunos inconvenientes para poder tener permiso hacia una entrevista en vista de que los funcionarios se encontraban en obligaciones de su cargo, regresamos al siguiente día en una hora que no interfiera con su tiempo de refrigerio o algún evento importante, donde oportunamente nos concedieron la entrevista que les planteamos y así terminamos concluimos con la organización de visitas a todas las entidades que teníamos que realizarles las entrevistas.

Los resultados de estas preguntas fueron transcritos personalmente, escuchando el audio de las entrevistas una a una y así registrando esta información digitalizada, lo que conlleva tener una información sólida y transparente de esta investigación.

El uso metodológico de instrumentos permite obtener un registro y medir los datos obtenidos en el desarrollo exploratorio de esta investigación, junto con este aspecto las entrevistas fueron estructuradas en base las ideas principales y las diferentes variables que derivan responsabilidades en los sectores y departamentos escogidos para optimizar el resultado del estudio.

El instrumentó utilizado como forma de recolección de información se implementó una guía de entrevistas estructurada que consiste en 6 preguntas para el área de talento humano y 5 preguntas para el área de sistemas y comunicaciones, elaborada a partir de las variables e indicadores definidos del estudio desarrollado, esta herramienta planteaba preguntas abiertas que permitieron indagar aspectos administrativos, tecnológicos y aplicativos relacionados al funcionamiento interno de  la marcación de asistencia biométrica en sus diferentes formas.

Las respuestas planteadas y guardadas fueron registradas de manera sistemática de transcripción y analizadas para así obtener una base de respuestas similares que coincidan

entre los tres GAD y la UPSE, lo que contribuyó a sustentar los resultados y conclusiones del estudio.

### 3.4 Tratamiento de la Información

Para el tratamiento de la información recopilada en las entrevistas use el método de transcripción, se implementó esta forma de transcripción porque las entrevistas se grabaron en audio y se guardaron, se procede a escuchar las preguntas y respuestas y transcribirlas una a una, cabe recalcar que se separó a todas las áreas donde fueron destinada las entrevistas, con la selección de las respuestas se empezó a contrastar las respuestas.

Concluyendo con los resultados se organizaron todas las entrevistas empleando una IA llamada Nootbooklm esta herramienta que ayudara a obtener un análisis profundo de las entrevistas comparándola con nuestra idea a defender teniendo una manera más agilizada y rápida de contrastar respuestas que asimilan una misma respuesta y así tener un texto interpretativo de la respuesta de todas las entrevistas realizadas.

### 3.5 Operalización de las variables

**Tabla 5. Operalización de las variables**

| TEMA | VARIABLE | CONCEPTUALIZACIÓN | DIMENSIONES | INDICADORES | ÍTEMS | INSTRUMENTOS |
|---|---|---|---|---|---|---|
| Marcación con datos biométricos en el sector público. | **Independiente** Implementación de sistema de marcación con datos biométricos en el sector público. | Proceso de adopción y uso de tecnologías que permiten registrar asistencia y horarios laborales de los empleados públicos mediante el uso de datos biométricos como huella dactilar, reconocimiento facial o lector QR. | -Tipo de tecnología biométrica.<br>-Proceso de registro y almacenamiento<br>-Consentimiento informado. | -Tipos de sistemas implementados.<br>Procedimientos de registro.<br>-Existencia de consentimiento informado. | • ¿Qué sistemas biométricos utiliza la institución?<br>• ¿Cuáles son las formalidades que aplica la entidad para recabar el consentimiento informado para el uso de la marcación biométrica?<br>• ¿En el ámbito de uso de nuevas tecnologías la entidad prevé nuevos métodos de registro que garanticen de mejor forma la protección de datos ¿<br>• ¿Ha habido incidentes reportados de filtración o mal uso de datos biométricos en su institución? ¿Cómo se manejaron?<br>• ¿La institución ejecuta auditorías y/o controles a los custodios de los datos biométricos de los empleados?□.¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores? | -Entrevistas. |
| | **Dependiente** Nivel de protección efectiva de los datos personales sensibles. | Grado en las que las instituciones públicas garantizan la seguridad, confidencialidad y correcto manejo de los datos biométricos recolectados de empleados conforme a la ley Orgánica de Protección de Datos Personales y a la Constitución del Ecuador. | -Seguridad en el almacenamiento | -Incidentes de filtración de datos. | • ¿Qué tecnologías biométricas se implementan en su institución y cómo se integran con los sistemas de gestión?<br>• ¿Qué protocolos técnicos de codificación, cifrado y seudonimización se utilizan para proteger los datos biométricos?<br>• ¿Cuáles son los principales riesgos técnicos identificados en el manejo de datos biométricos y cómo se mitigan?<br>• ¿Cómo se asegura la confidencialidad y la integridad de la información biométrica frente a posibles ataques cibernéticos?<br>• ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores? | -Entrevistas. |
| | | | -Protocolos de acceso y modificación. | -Existencia de políticas de protección. | | |
| | | | -Medidas de protección legal | -Capacitación del personal. | | |

# CAPÍTULO IV

## RESULTADOS Y DISCUSIÓN

### 4.1 Análisis, interpretación y discusión de resultados

**Entrevistas realizadas a profesionales del área de Talento Humano**

**Entrevista No. 1**

**Santa Elena**

**Nombre del entrevistado:** Ing. Karen Rivera González.

**Cargo:** Directora de Talento Humano del Gobierno Autónomo Descentralizado Municipal de Santa Elena

1. ¿Qué sistemas biométricos utilizan para el registro de asistencia en su institución (huella dactilar, reconocimiento facial, lector QR u otros)?

Actualmente, en esta administración hacemos el control de las marcaciones por medio del biométrico, tiene a su vez dos opciones que es el reconocimiento facial por parte de cada uno de los servidores públicos, funcionarios, y también el registro de la huella dactilar.

2. ¿Cuáles son las formalidades que aplica la entidad para recabar el consentimiento informado para el uso de la marcación biométrica?

En cuanto a las obligaciones de las marcaciones una vez que ingresa el personal a tener relación laboral dentro de la institución se le indica a través del departamento de talento humano, cuál serían sus obligaciones, actualmente nosotros manejamos las obligaciones de cuatro marcaciones dentro del horario laboral, lo que corresponde a la marcación de ingreso, la marcación de entrada y salida del almuerzo y la marcación de la culminación de la jornada. En muchas ocasiones, también a través de un documento de confidencialidad para poder tener la certeza de qué se maneja las marcaciones durante los cinco días, es decir las 40 horas laborales.

3 ¿En el ámbito de uso de nuevas tecnologías la entidad prevé nuevos métodos de registro que garanticen de mejor forma la protección de datos?

Sí, se prevé nuevas actualizaciones en el campo de la seguridad biométrica.

4 ¿Ha habido incidentes reportados de filtración o mal uso de datos biométricos en su institución? ¿Cómo se manejaron?

Como antecedente en el año 2018 en este municipio hubo un hackeo de información, debido a que nosotros manejamos los servidores y se perdió información, se puede decir desde el 2018 hacia atrás hace años atrás, pero se ha implementado nuevamente el tema del sistema, o poder tener esas restricciones a través del departamento del sistema para evitar nuevamente que nos ocurra.

5 ¿La institución ejecuta auditorías y/o controles a los custodios de los datos biométricos de los empleados?

Como dirección de talento humano trabajamos directamente con la dirección de sistemas, el director de tecnología en sistema es el encargado de poder controlar a través de los servidores que nosotros manejamos y las líneas del proxy para evitar este tipo de incidentes.

6. ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

A través del reglamento interno de talento humano, a través de su artículo 25, que indica el registro y control de asistencia, manejamos obligatoriamente el registro, el ingreso también de la información al mismo sistema, es decir, en los biométricos que nosotros tenemos al aumento se registra dentro del equipo y nosotros hacemos la descarga a través de un pendrive, esa información es ingresada al sistema mediante claves, y una vez que se registra se imprime las marcaciones y constantemente se hace el control de las asistencias, a su vez, una vez verificado que existan atrasos, faltas o servicios y comisiones que no se han cumplido durante los primeros cinco días que la normativa indica de espera pues se procede a realizar amonestaciones, llamadas de atención, entre otras variedades de memos.

**Entrevista No. 2**

**La Libertad**

**Nombre del entrevistado:** Estefanía Moreno Ponce.

**Cargo:** Directora de Talento Humano del Gobierno Autónomo Descentralizado Municipal de Libertad.

1. ¿Qué sistemas biométricos utilizan para el registro de asistencia en su institución (huella dactilar, reconocimiento facial, lector QR u otros)?

Sólo se utiliza el sistema de huella dactilar.

2. ¿Cuáles son las formalidades que aplica la entidad para recabar el consentimiento informado para el uso de la marcación biométrica?

Cuando ingresan a laborar al municipio, se le informa que la forma de marcar es por medio de la huella dactilar o en su defecto personas que tiene problemas con la huella dactilar, se realiza una valoración médica y el mismo médico de seguridad y salud, verifica que la persona tiene algún problema con la huella dactilar y se le procede a dar un código, pero esto no aplica a todos sólo se aplica a las personas con esta particularidad.

3 ¿En el ámbito de uso de nuevas tecnologías la entidad prevé nuevos métodos de registro que garanticen de mejor forma la protección de datos?

Se tiene muchas alternativas en las que se está esperando las respectivas asignaciones con el presupuesto al municipio para poder avanzar con los mismos.

4 ¿Ha habido incidentes reportados de filtración o mal uso de datos biométricos en su institución? ¿Cómo se manejaron?

No.

5 ¿La institución ejecuta auditorías y/o controles a los custodios de los datos biométricos de los empleados?

Si.

6. ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

No existen protocolos.

**Entrevista No. 3**

**Salinas**

**Nombre del entrevistado:** Lcdo. Vinicio Benavides.

**Cargo:** Directora de Talento Humano del Gobierno Autónomo Descentralizado Municipal de Salinas.

1. ¿Qué sistemas biométricos utilizan para el registro de asistencia en su institución (huella dactilar, reconocimiento facial, lector QR u otros)?

Contamos con biométricos de reconocimiento facial.

2. ¿Cuáles son las formalidades que aplica la entidad para recabar el consentimiento informado para el uso de la marcación biométrica?

Se utilizan políticas internas de la institución.

3 ¿En el ámbito de uso de nuevas tecnologías la entidad prevé nuevos métodos de registro que garanticen de mejor forma la protección de datos?

El departamento de sistemas siempre presenta informa de las nuevas tecnologías, dependerá del municipio de salinas que en el presupuesto tomen en consideración dichas propuestas.

4 ¿Ha habido incidentes reportados de filtración o mal uso de datos biométricos en su institución? ¿Cómo se manejaron?

Hasta el momento no se han presentado inconvenientes.

5 ¿La institución ejecuta auditorías y/o controles a los custodios de los datos biométricos de los empleados?

La información queda grabada en el departamento de sistemas, auditoria como tal no se realiza ya que no se presentan novedades.

6. ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

Dentro de la ley que nosotros manejamos como servidores públicos, los mismo son responsable que todo lo que maneja la institución no puede ser expuesto ni sacado, ya que es exclusividad de la entidad.

**Entrevista No. 4**

**Universidad Estatal Península de Santa Elena**

**Nombre del entrevistado:** Leonardo Del Pezo.

**Cargo:** Técnico de Sistema en el Área de Departamento Humano.

1. ¿Qué sistemas biométricos utilizan para el registro de asistencia en su institución (huella dactilar, reconocimiento facial, lector QR u otros)?

Al ser una institución de educación superior utilizamos dos sistemas de marcación: el sistema de marcación y el de huella dactilar.

2. ¿Cuáles son las formalidades que aplica la entidad para recabar el consentimiento informado para el uso de la marcación biométrica?

Nosotros como institución no manejamos un documento formal que certifique el consentimiento del funcionario.

3 ¿En el ámbito de uso de nuevas tecnologías la entidad prevé nuevos métodos de registro que garanticen de mejor forma la protección de datos?

Sí, se tiene planeado y planificado la adquisición de mejores relojes biométricos, porque los que tenemos están desactualizados.

4 ¿Ha habido incidentes reportados de filtración o mal uso de datos biométricos en su institución? ¿Cómo se manejaron?

No, hasta el momento no hemos tenido problemas con la filtración de datos.

5 ¿La institución ejecuta auditorías y/o controles a los custodios de los datos biométricos de los empleados?

La instrucción como tal no realiza no realiza la auditorias, pero contraloría si realiza auditoras hacia nosotros.

6. ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

No se cuenta con una regulación en la actualidad.

**Entrevistas realizadas a profesionales del área de las Tics**

**Entrevista No. 1**

**Santa Elena**

**Nombre del entrevistado:** Ernesto Mence Figueroa.

**Cargo:** Director de Informática y Tecnología del Gobierno Autónomo Descentralizado Municipal de Santa Elena.

1. ¿Qué tecnologías biométricas se implementan en su institución y cómo se combinan con los sistemas de control?

Nosotros utilizamos tecnologías biométricas, reconocimiento facial y huella dactilar.

2. ¿Qué protocolos técnicos de codificación, cifrado y seudonimización se utilizan para proteger los datos biométricos?

Los datos biométricos que utilizamos es encriptación y la huella dactilar de cada persona.

3 ¿Cuáles son los principales riesgos técnicos identificados en el control de datos biométricos y cómo se reducen?

Uno de los principales riesgos es al momento de la marcación es cuando el usuario registra su ingreso o salida, se descarga el archivo del biométrico y se lo carga el sistema de control de asistencias en ese laxo hay un riesgo que pueda sufrir alguna modificación y nosotros prevenimos eso mediante los dos administradores del biométrico.

4 ¿Cómo se garantiza la confidencialidad y la integridad de la información biométrica frente a posibles ataques cibernéticos?

La seguridad biométrica la maneja el dispositivo como tal, no hay manera que exista un ataque cibernético al reloj, ya que este opera independientemente de datos del municipio.

5 ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

Nos regimos a ley de protección de datos del Ecuador, pero muy aparte de eso tenemos una ordenanza de protección de datos de la información que maneja el municipio, la cual está aprobada en primeras instancias por parte del consejo municipal y falta de aprobar la segunda instancia, una vez aprobado esto se va el registro oficial para su cumplimiento.

**Entrevista No. 2**

**La Libertad**

**Nombre del entrevistado:** John Reyes Lindao.

**Cargo:** Coordinado de Sistemas y Recursos Tecnológicos.

1. ¿Qué tecnologías biométricas se implementan en su institución y cómo se combinan con los sistemas de control?

En la actualidad sólo se tiene marcación con huella digital para la asistencia antes durante y después del día laborable y la integración se hace vía Bach, es decir que se exporta la información y la ingresamos al sistema administrativo.

2. ¿Qué protocolos técnicos de codificación, cifrado y seudonimización se utilizan para proteger los datos biométricos?

El dato biométrico que se tiene en la actualidad sólo es el código y la cédula no hay datos biométricos como rasgos faciales, por lo tanto, no se utiliza codificación.

3 ¿Cuáles son los principales riesgos técnicos identificados en el control de datos biométricos y cómo se reducen?

Las dependencias externas sólo están enlazadas vía antena, se tiene códigos duplicados de relojes biométricos, es decir que el biométrico uno puede existir otro biométrico.

4 ¿Cómo se garantiza la confidencialidad y la integridad de la información biométrica frente a posibles ataques cibernéticos?

Los relojes biométricos son la única identificación que se tiene en este momento, sólo están en una VPN interno y estos no cuentan con servicio a internet, por lo tanto, no hay riego de un ataque cibernético.

5 ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

Si se tiene protocolos, pero ahí no se almacenan los datos biométricos. Los datos biométricos se almacenan dentro de los propios biométricos en sus historiales y se respalda en la aplicación de los biométricos.

**Entrevista No. 3**

**Salinas**

**Nombre del entrevistado:** Ing. Wellington Robbis.

**Cargo:** Director del Departamento de Sistemas.

1. ¿Qué tecnologías biométricas se implementan en su institución y cómo se combinan con los sistemas de control?

Se tiene dos tipos de biometría, en la actualidad, la facial y la dactilar. Todos se enlace con el sistema integrado y administrativo.

2. ¿Qué protocolos técnicos de codificación, cifrado y seudonimización se utilizan para proteger los datos biométricos?

Toda nuestra base de datos entripado por algún tipo de virus (no entiendo el audio en esta parte).

3 ¿Cuáles son los principales riesgos técnicos identificados en el control de datos biométricos y cómo se reducen?

Primero es el daño del biométrico, pero lo mitigamos descargando todas las marcaciones viables, tanto en las diferentes jornadas que hay de los trabajadores y obreros.

4 ¿Cómo se garantiza la confidencialidad y la integridad de la información biométrica frente a posibles ataques cibernéticos?

El entrevistado aseguro que la pregunta era compleja, pero se maneja la seguridad informática la nueva ley de protección de datos que tienen a nivel del Ecuador y de manera interna por protocolo respaldo de intervención. Se realiza Cup y la migración de una base de datos a otra que tienen ubicada en otra locación.

5 ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

Manejamos tiempo de respaldo de información, la seguridad de la red interna y la red externa manejan un ERL para todos los equipos informáticos y a nivel de respaldo de información hacia el espejo que se tiene de la base de datos para todos los servidores.

**Entrevista No. 4**

**Universidad Estatal Península de Santa Elena**

**Nombre del entrevistado:** Francisco Bolívar Quijano Benavides.

**Cargo:** Analista de soporte redes e infraestructura.

1. ¿Qué tecnologías biométricas se implementan en su institución y cómo se combinan con los sistemas de control?

Lectura biométrica, uso de la huella dactilar para la administración correspondiente a lo administrativo y servicios generales, lo que es para docencia es con lector QR con su respectiva tarjeta o identificativo.

2. ¿Qué protocolos técnicos de codificación, cifrado y seudonimización se utilizan para proteger los datos biométricos?

El mismo software de los biométricos encripta, o te descifra la información que va a entrar al biométrico, por ejemplo, la lectura de la huella. Aunque la propia institución ha desarrollado un software.

3 ¿Cuáles son los principales riesgos técnicos identificados en el control de datos biométricos y cómo se reducen?

El único riesgo es con la lectura del QR. Puesto que se puede intercambiar las tarjetas.

4 ¿Cómo se garantiza la confidencialidad y la integridad de la información biométrica frente a posibles ataques cibernéticos?

Dentro de la estructura de red de comunicaciones que se tienen institución seguridad se maneja la seguridad y los biométricos están dentro de una red propia solo de biométricos y si un agente externo quiere ingresar a la información no lo podrá hacer gracias a la seguridad que brinda el equipo de trabajo, el acceso solo lo tienen los que administra la aplicación de marcaciones que en este caso sería el departamento de talento humano.

5 ¿Existen protocolos, normas o reglamentos específicos donde se regulen la protección de los datos de los servidores?

El departamento de talento humano es el que maneja toda esa información.

### 4.2 Verificación de la idea a defender

La idea a defender, tal como se establece en la investigación, es que los sistemas de marcación con datos biométricos implementados en el sector público de Santa Elena presentan deficiencias en la protección, almacenamiento seguro y adecuado consentimiento informado, lo que compromete al derecho constitucional a la protección de datos personales de los funcionarios públicos.

Los resultados de las entrevistas realizadas a los profesionales de Talento Humano y del Departamento de Sistemas y Comunicaciones de los GAD de Santa Elena, La Libertad y Salinas, así como de la Universidad Estatal Península de Santa Elena (UPSE), confirman plenamente esta idea central, las respuestas obtenidas demuestran una falta de conocimiento y una nula existencia de protocolos que revelan deficientes críticas en la protección y el almacenamiento de los datos sensibles de los servidores, se argumenta esta idea basándose en el contraste de la normativa legal vigente con las prácticas operacionales del sector público en Santa Elena, evidenciando las tres deficiencias principales como la falta de consentimiento adecuado, el almacenamiento inseguro y la falta de protocolos de protección.

**1. Marco normativo y la naturaleza sensible de los datos biométricos.**

La protección de datos se refiere a los derechos que tienen las personas sobre su información, incluyendo obligaciones legales y éticas al compartir datos personales. Los datos personales son cualquier información que pueda revelar la identidad de una persona viva, ya sea por sí sola o vinculada a otros datos.

En el contexto ecuatoriano, la protección de datos es un derecho fundamental, la Constitución de la República garantiza el derecho a la protección de datos de carácter personal, que comprende el acceso y la decisión sobre dicha información, solicitando la autorización del titular o mandato de ley para su recolección, archivo, procesamiento, distribución o difusión, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece principios y mecanismos para garantizar el ejercicio de este derecho.

El Convenio modernizado para la protección de las personas con respecto al tratamiento de datos personales-128 (2018) establece que el tratamiento de datos biométricos que identifican de forma única a una persona solo se permitirá si la ley contempla garantías

adecuadas que protejan contra los riesgos, en particular el riesgo de discriminación, que este tratamiento pueda presentar para los derechos y libertades fundamentales del interesado.
La implementación de sistemas de reconocimiento facial o huella dactilar en el sector público, como los utilizados por los GAD de Santa Elena y La Libertad, requiere, por lo tanto, el máximo nivel de seguridad y un consentimiento informado explícito.

**2. Deficiencias en el consentimiento informado**

Una de las principales fallas identificadas en la tesis es la ausencia de un adecuado consentimiento informado.
Los testimonios de los directores de Talento Humano en las instituciones de Santa Elena revelan prácticas informales o dependientes de reglamentos internos insuficientes:

- Universidad Estatal Península de Santa Elena (UPSE): El técnico de sistema en el Área de Departamento Humano admitió claramente que la institución no maneja un documento formal que certifique el consentimiento del funcionario para el uso de la marcación biométrica.
- GAD de La Libertad: Se indica al personal al momento de ingresar que la forma de marcar es con la huella dactilar. Si existen problemas con la huella, se realiza una valoración médica para asignar un código, pero esto solo aplica a las personas con esa particularidad, donde no se menciona un proceso formal de consentimiento informado.
- GAD de Salinas: se recurre a políticas internas de la institución.
- GAD de Santa Elena: se informa sobre las obligaciones de cuatro marcaciones y en muchas ocasiones se utiliza un documento de confidencialidad, estas respuestas confirman que el requisito fundamental de la normativa que es la recolección de datos personales, requiera la autorización del titular y no se cumple de manera formal y estandarizada, el simple hecho de informar o depender de políticas internas o usar un documento de confidencialidad en muchas ocasiones no constituye la garantía legal y específica requerida para el tratamiento de datos sensibles como los biométricos.

**3. Deficiencias en la protección y almacenamiento seguro falta de protocolos.**

La idea a defender se sustenta firmemente en la evidente falta de protocolos, normas o reglamentos específicos que regulen la protección de datos de los servidores.

Al preguntar si existen protocolos específicos, las respuestas del sector público de Santa Elena son contundentes:

- GAD de La Libertad: la directora de Talento Humano afirmó que no existen protocolos. El Coordinador de Sistemas señaló que sí existen protocolos, pero en ellos no se almacenan los datos biométricos, los cuales se guardan en los propios biométricos y se respaldan en la aplicación.
- UPSE**:** se confirmó que no se cuenta con una regulación en la actualidad.
- En otras instituciones, las referencias son vagas o dependen de regulaciones generales que no abordan específicamente la protección de datos biométricos.
- GAD de Santa Elena**:** el director de Informática y Tecnología mencionó que se rigen por la Ley de Protección de Datos del Ecuador, pero que una ordenanza de protección de datos de la información del municipio está solo en proceso de aprobación (pendiente de segunda instancia y registro oficial). La directora de Talento Humano mencionó el artículo 25 del reglamento interno, que se centra en el registro y control de asistencia, no en la protección específica de los datos en sí.

Esta ausencia de una regulación interna específica, junto con la variación en los mecanismos de seguridad, expone la vulnerabilidad de la información:

• En el GAD de Santa Elena, existió un antecedente de un hackeo de información en 2018, resultando en la pérdida de datos y obligando a la implementación posterior de restricciones a través del departamento de sistemas, esto explica el riesgo real en el almacenamiento de datos sensibles.

- En el manejo de riesgos el director de Informática de Santa Elena identificó que el peligro principal se presenta cuando el archivo del biométrico es descargado y cargado al sistema de control de asistencias admitiendo que en ese lapso podría haber una modificación, donde la Ley exige que las instituciones públicas garanticen la seguridad, confidencialidad y correcto manejo de los datos biométricos recolectados conforme a la Constitución y la Ley de Protección de Datos Personales, la conclusión de la investigación es que la nula existencia o la insuficiencia de estos protocolos confirma la tesis de la deficiencia en la protección y almacenamiento seguro.

**4. Deficiencias en auditorías y controles.**

Finalmente, la debilidad en los mecanismos de control interno agrava la vulnerabilidad del sistema, reforzando la idea de deficiencia en la protección.

- GAD de Salinas indicó que las auditorías no se realizan ya que no se presentan novedades.
- UPSE confirmó que la institución como tal no realiza auditorías, aunque sí las realiza Contraloría.

Si bien el GAD de La Libertad afirmó realizar auditorías, la práctica de otras instituciones de no ejecutar auditorías o de basarse únicamente en la ausencia de "novedades" muestra una actitud pasiva en la gestión de la seguridad. La falta de control riguroso sobre los custodios de los datos biométricos y la ausencia de auditorías periódicas por parte de la propia entidad compromete la integridad y la confidencialidad de la información, especialmente aquella que se encuentra almacenada y respaldada en los propios dispositivos y aplicaciones internas.

En resumen, el contraste de las obligaciones legales internacionales y nacionales (Constitución, LOPDP) con las prácticas documentadas en las entrevistas (falta de consentimiento formal en UPSE, ausencia de protocolos en La Libertad y UPSE, y el antecedente de un hackeo en Santa Elena) demuestra que existe un incumplimiento sistemático en la garantía del derecho a la protección de datos personales de los funcionarios públicos de Santa Elena, validando completamente la idea a defender

En este sentido por medio del contraste de respuestas recabadas de las entrevistas planteadas a los profesionales tanto de talento humano y del departamento de sistema y comunicación de los diferentes GAD de la provincia de Santa Elena y además incluyendo a la Universidad Estatal Península de Santa Elena se concluye que, sí se cumple con la idea a defender que se planteó, porque las respuestas de los entrevistados dejan ver laménteme la falta de conocimiento e incluso una nula existencia de un protocolo dejando ver la deficiencia en la protección, almacenamiento seguro y adecuado de los datos.

**Conclusiones**

- La investigación confirma la deficiencia sistemática en la obtención de un consentimiento informado adecuado y formal para el uso de datos biométrico, las practicas operacionales en las instituciones, como la Universidad Estatal Península de Santa Elena y los Gobiernos Autónomos Descentralizados, depende de reglamentos internos insuficientes, de la simple comunicación verbal o el uso ocasional de documentos de confidencialidad esta informalidad no cumple con el requisito fundamental de la normativa que exige la autorización específica del titular para la recolección de datos sensibles.
- Se deduce que la tesis se sustenta firmemente en la nula existencia o insuficiencia critica de protocolos, normas o reglamentos internos específicos que regulen la protección y almacenamiento seguro de datos biométricos de los servidores, entidades como el GAD de La Libertad y la UPSE confirmaron la inexistencia de protocolos o regulaciones en la actualidad, esta carencia sumada a la variación de mecanismos de seguridad expone la vulnerabilidad de la información sensible.
- Existe una vulnerabilidad operacional latente y confirmada en el manejo de los datos reforzada por antecedentes de riesgo como el hackeo de información que sufrió el GAD de Santa Elena en el año 2018, además el director de informativa de santa Elena admitió que el principal riesgo de seguridad ocurre cuando el archivo biometría es descargado y cargado al sistema de control de sistema permitiendo una posible modificación en ese lapso.
- La investigación revela una debilidad en los mecanismos de control interno debido a una actitud pasiva en la gestión de la seguridad, instituciones como el GAD de Salinas y la UPSE indicaron que no realizan auditorías internas o que se basan en la ausencia de novedades, comprometiendo la integridad de la información que se encuentra almacenada y respaldada en dispositivos y aplicaciones internas.

**Recomendaciones**

- Implementar un documento formal especifico y estandarizado de consentimiento informado para el tratamiento de datos biométricos, que debe ser firmado obligatoriamente por el funcionario, este documento debe garantizar que la recolección, archivo y procesamiento de datos biométricos se realicen solo con la autorización expresa del titular cumpliendo así con las garantías legales requeridas para datos de carácter sensibles.
- Elaborar, aprobar y socializar urgentemente una regulación interna especifica y detallada (como protocolos, ordenanzas o reglamentos) que aborde exclusivamente la protección de datos biométricos esta normativa debe asegurar que se establezcas mecanismos para garantizar la seguridad, confidencialidad y el correcto manejo de los datos recolectados alineándose con la Ley Orgánica de la Protección de Datos Personales.
- Fortalecer auditorias que implementen mecanismos de seguridad técnicas en los puntos de transferencia y almacenamiento, especialmente en el proceso de descarga y carga de los archivos biométricos hacia el sistema de control de asistencia, es crucial implementar medidas que mitiguen el riesgo de alteración o perdida de datos durante esta fase operacional garantizando la seguridad y confidencialidad exigida por la ley.
- Establecer un programa obligatoria y periódico de auditorías internas para los sistemas de marcación biométricas y los custodios de datos, estas auditorías deben ser realizadas por la propia entidad más allá de los controles externos, para evaluar de manera proactiva la gestión de la seguridad, la integridad de información y el cumplimiento de los protocolos establecidos, evitado depender de la simple ausencia de incidentes.

## Bibliografía


Silva Gallinato, M. P. (10 de 2018). *Principio de taxatividad,Constitución y proceso penal.* https://www2.tribunalconstitucional.cl/wp-content/uploads/2022/03/Nelson-Pozo-Silva-Principio-de-Taxitividad-Constitucio%CC%81n-y-proceso-penal.pdf

ACESS. (10 de 9 de 2022). *Consentimiento informado* . ACESS: http://www.acess.gob.ec/consentimiento-informado/

Administrador. (24 de 5 de 2023). https://www.santaelena.gob.ec/index.php/links/politica-de-proteccion-de-datos-personales

Agencia Española Protección datos. (2024). *LA **K**-ANONIMIDAD COMO MEDIDA DE LA PRIVACIDAD.* Madrid. https://www.aepd.es/guias/nota-tecnica-kanonimidad.pdf

Aratek. (4 de 12 de 2023). *Seguridad biométrica: el futuro de la seguridad personal y pública*. https://www.aratek.co/es/news/biometric-security-the-future-of-personal-and-public-safety

Arias, B. (2025). *La privacidad en el ámbito laboral en Chile: la carencia de protección para los datos biométricos.* Chile: UNIVERSIDAD DE CHILE.

AUTELSI . (2021). *Estudio Suplantación Identidad Digital.* https://autelsi.es/pdfs/documentos-de-autelsi/suplantacion-identidad/Estudio_Suplantacion_Identidad_AUTELSI.pdf

Betancourt, J. (2018). https://www.jacquelinebetancourt.com/single-post/2019/03/04/Mejora-Continua-Excelencia-a-nuestro-alcance

Bonilla, M. (24 de 3 de 2025). *La SPDP establece que no es legítimo el uso de datos biométricos para el registro de asistencia laboral*. NMS: https://nmslaw.com.ec/blog/2025/03/24/spdp-datos-biometricos-registro-asistencia-laboral-ecuador/

Buenning, M. (18 de 8 de 2025). *Plan de Protección de Datos: Guía y 8 pasos para su creación.* NinjaOne: https://www.ninjaone.com/es/blog/plan-de-proteccion-de-datos-pasos-para-la-creacion/#

Bustamante Fabara. (2025). *Uso de Sistemas Biométricos para el Registro de Asistencia de Trabajadores.* https://bustamantefabara.com/uso-de-sistemas-biometricos-para-el-registro-de-asistencia-de-trabajadores/#:~:text=Naturaleza%20de%20los%20datos%20biom%C3%A9tricos,legitimaci%C3%B3n%20establecida%20en%20la%20LOPDP.

Castillo, A. (29 de 8 de 2024). *Biometría por huella dactilar: La forma más antigua de identificación biométrica*. Verázial: https://www.verazial.com/biometria-por-huella-dactilar-la-forma-mas-antigua-de-identificacion-biometrica/

Castro, A. (1 de 6 de 2024). *Cyber War*. https://cyberwarmag.com/privacidad-datos-sector-publico-transparencia-seguridad/

CEPAL. (5 de 1 de 2024). *Biblioguias: Gestión de datos de investigación: protección de los datos*. https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Cheon, S. (31 de 3 de 2025). *El Estado de la Tecnología de Reconocimiento Facial en 2025: Precisión, Rendimiento y Tendencias Futuras*. ANDOPEN: https://andopen.co.kr/es/el-estado-de-la-tecnologia-de-reconocimiento-facial-en-2025-precision-rendimiento-y-tendencias-futuras/

COE Search - CM. (18 de 5 de 2018). https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Constitución de la Republica del Ecuador. (2008). *Articulo 11 TÍTULO II*. LEXIS. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Constitución de la República del Ecuador. (21 de 5 de 2008). *articulo 66 #19 (capitulo) sexto*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Córdova-Real, J. L. (01 de 12 de 2023). Técnicas de anonimización y pseudonimización en la protección de datos personales. *Journal Scientifi MQR Investigar*, 235. https://doi.org/https://doi.org/10.56048/MQR20225.8.1.2024.204-235

Corona, J. L. (2018). *INVESTIGACIÓN CUALITATIVA: FUNDAMENTOS EPISTEMOLÓGICOS, TEÓRICOS y METODOLÓGICOS*. https://www.redalyc.org/journal/5257/525762351005/html/#:~:text=La%20investigaci%C3%B3n%20cualitativa%20es%20un%20paradigma%20emergente%20que%20sustenta%20su,ser%20pensante%2C%20respecto%20a%20los

ECIJA. (21 de 9 de 2022). *Ecuador: Biometría y protección de datos personales en el marco de la legislación ecuatoriana*. ECIJA: https://www.ecija.com/actualidad-insights/ecuador-biometria-y-proteccion-de-datos-personales-en-el-marco-de-la-legislacion-ecuatoriana/

ESIC University. (7 de 2023). ¿Qué es la codificación de datos?: tipos y ejemplos. https://www.esic.edu/rethink/marketing-y-comunicacion/que-es-codificacion-datos-tipos-ejemplos-c

Espinoza, G. (12 de 9 de 2024). *Expreso*. .https://www.expreso.ec/ciencia-y-tecnologia/filtraciones-datos-2024-1-500-millones-registros-expuestos-213387.html

European Union Agency For Cybersegurity. (3 de 2022). *Enisa.* https://www.aepd.es/documento/tecnicas-seudonimizacion-sector-sanitario-enisa.pdf

F. de Marcos, I. D. (2022). *Diccionario de Protección de Datos Personales.* https://secihti.mx/wp-content/uploads/transparencia/proteccion_datos_personales/informacion_relevante/guias_y_materiales/Diccionario_de_Proteccion_de_Datos_Personales.pdf

GADPSE. (24 de 5 de 2023). https://www.santaelena.gob.ec/index.php/11-proyectos/santa-elena-digital

Garrija, D. A. (2004). *Tratamiento de datos personales y derechos fundamentales.* Madrid: Librería-Editorial Dykinson.

Godoy, L. N. (5 de 8 de 2024). El iris es un dato biométrico de alto riesgo. *El Comercio*. https://www.elcomercio.com/opinion/iris-dato-biometrico-alto-riesgo-lorena-naranjo-columnista.html

Innovatrics. (3 de 8 de 2023). *Biometric Identification - Innovatrics*. Innovatrics: https://www.innovatrics.com/glossary/biometric-identification/

La Hora. (18 de 12 de 2024). *Funcionarios del IESS son investigados por suplantar identidades de jubilados para hacer préstamos.* https://www.lahora.com.ec/pais/funcionarios-del-iess-son-investigados-por-suplantar-identidades-de-jubilados-para-hacer-prestamos/

Ley Orgánica de Protección de Datos. (2021). *Articulo 4 (Capitulo I).* LEXIS. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley Orgánica de Protección de Datos. (2021). *Articulo 43 (capitulo V).* LEXIS. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley Orgánica de Protección de Datos. (2021). *Ley Orgánica de Protección de Datos.* Lexis. https://doi.org/https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley Orgánica de Protección de Datos Personales. (2021). *Articulo 1 (Capitulo I).* LEXIS. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley Orgánica de Protección de Datos Personales. (2021). *Articulo 34 (capitulo V).* LEXIS. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Lezcano, J. M. (23 de 6 de 2023). La interoperabilidad en la administración de justicia bonaerense y la calidad del dato como elemento clave para el acceso a derechos. *SADIO EJS*, *22*(2), 261. https://doi.org/10.24215/15146774e034

Maciejewsk, M. (4 de 8 de 2025). *La protección de los datos personales.* https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/es/FTU_4.2.8.pdf

Martínez González , M. M., y De Valladolid Escuela De Ingeniería Informática De, U. (2021). *Aplicación de la técnica de K-anonimización sobre bases de datos relacionales.* Universidad de Valladolid: https://uvadoc.uva.es/handle/10324/50409

Mera Moreira, E. (21 de 3 de 2025). Diario Expreso. *Empleadores en Ecuador deben evitar uso de datos biométricos, dice Superintendencia*. https://www.expreso.ec/actualidad/empleadores-ecuador-deben-evitar-datos-biometricos-dice-superintendencia-235909.html

Ministerio de Telecomunicaciones y de la Información. (1 de 3 de 2024). *ACUERDO Nro. MINTEL-MINTEL-2024-0003.* https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Miranda, J. (22 de 1 de 2024). *SCM LATAN*. https://scmlatam.com/que-es-la-biometria-ventajas-en-control-de-asistencia/#elementor-toc __heading-anchor-7

Monforte, E. (23 de 11 de 2023). *Datos biométricos: qué son y para qué se utilizan.* Camerfirma: https://www.camerfirma.com/datos-biometricos-que-son-para-que-se-utilizan/#Control_de_acceso

Palma, C. L. (03 de 05 de 2019). *Visionario Digital.* https://doi.org/10.33262/visionariodigital.v3i3.608

Pesántez, S. (21 de 11 de 2023). *RESUMEN LEY DE PROTECCIÓN DE DATOS Y REGLAMENTO.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Resumen.pdf

Pires, R. (3 de 6 de 2022). *Rock Content*. https://rockcontent.com/es/blog/que-es-un-cronograma/

Ponce, L. (2025). *Pwc*. https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html

PowerData. (2025). *GDPR: lo que debes saber sobre el Reglamento General de Protección de Datos*. PowerData: https://www.powerdata.es/gdpr-proteccion-datos

Reglamento a la Ley Orgánica de Protección de Datos Personales. (08 de 11 de 2023). https://nmslaw.com.ec/blog/2023/11/08/ecuador-reglamento-lopdp-2023/

Reglamento del Parlamento Europeo. (04 de 06 de 2016). *EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Roldán, A. L. (04 de 05 de 2024). *MASSIENCIE*. https://www.masscience.com/ley-organica-proteccion-datos-personales-ecuador/

Rosas-Lanas, G., y Pila-Cárdenas, G. (30 de 1 de 2023). Protección de datos personales en Ecuador. *VISUAL REVIEW International Visual Culture Review / Revista Internacional de Cultura Visual, 13*(2), 3. https://doi.org/10.37467/revvisual.v10.4568

Salusplay. (2025). *Las Variables de Investigación*. Salusplay: https://www.salusplay.com/apuntes/apuntes-metodologia-de-la-investigacion/tema-2-las-variables-de-investigacion

Santander. (2024). *Santander*. https://www.bancosantander.es/glosario/confidencialidad-informacion#:~:text=La%20confidencialidad%2C%20en%20inform%C3%A1tica%2C%20es,est%C3%A1%20almacenada%20o%20en%20tr%C3%A1nsito.

Sanz, F. (2016). Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. *Ius et Praxis*(1), 323 - 376. https://doi.org/http://dx.doi.org/10.4067/S0718-00122016000100010

Saúco, A. (9 de 6 de 2025). *Protección de datos e IA en Europa: retos y oportunidades*. Facephi: https://facephi.com/proteccion-de-datos-e-inteligencia-artificial-en-europa-el-gran-reto-legal-del-futuro/

Secureframe. (2025). *Métricas y KPI de gobernanza de datos*. https://secureframe.com/hub/grc/data-governance-metrics

Sieiro, C. Á. (26 de 06 de 2019). *PRODAT*. https://www.prodat.es/blog/a-vueltas-con-la-anonimizacion-hablamos-de-la-k-anonimidad/

Software Público Ecuador. (14 de 6 de 2019). *Aplicación de marcaciones*. https://www.softwarepublico.gob.ec/catalogo-de-software-publico-nacional/aplicacion-de-marcaciones-_1/

Solove, D. J. (5 de 5 de 2008). *GW LAW*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

Superintendencia de Protección de Datos Personales. (21 de 1 de 2024). *SPDP*. https://spdp.gob.ec/consultasatendidas/

Uguina, J. (22 de 7 de 2024). El “Big Bang” de la biometría laboral. De la huella dactilar a los neurodatos. *Labos Revista de Derecho del Trabajo y Protección Social, 5*(2), 13. https://doi.org/10.20318/labos.2024.8749

Unda, D. (2 de 5 de 2024). *Meythaler & Zambrano*. https://www.meythalerzambranoabogados.com/post/implicaciones-del-uso-de-huellas-digitales-en-el-control-horario

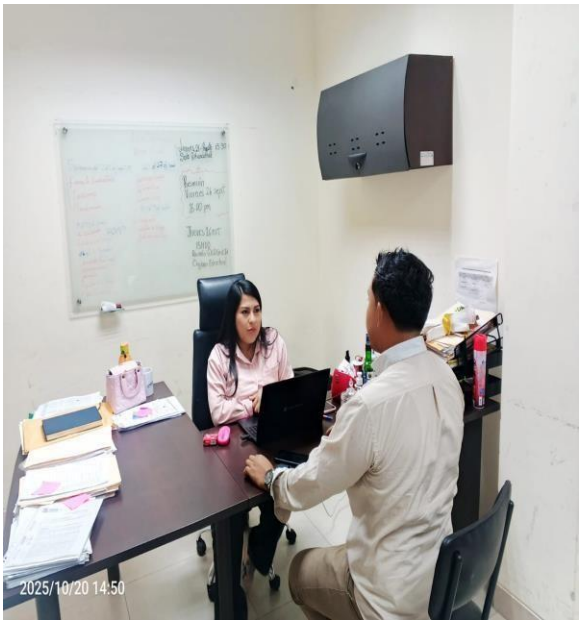
UTPL. (15 de 1 de 2025). *Innovación tecnológica para la protección de datos personales en Ecuador*. UTPL-BLOG: https://noticias.utpl.edu.ec/innovacion-tecnologica-para-la-proteccion-de-datos-personales-en-ecuador

Valle, H. Q.-d. (7 de 6 de 2022). *CENTER FOR DEMOCRACY & TECHNOLOGY*. https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/

## ANEXOS

Anexo 1

Entrevistas al personal de talento humano y sistemas del municipio del cantón Santa Elena



Anexo 2

Entrevistas al personal de talento humano y sistemas del municipio del cantón La Libertad

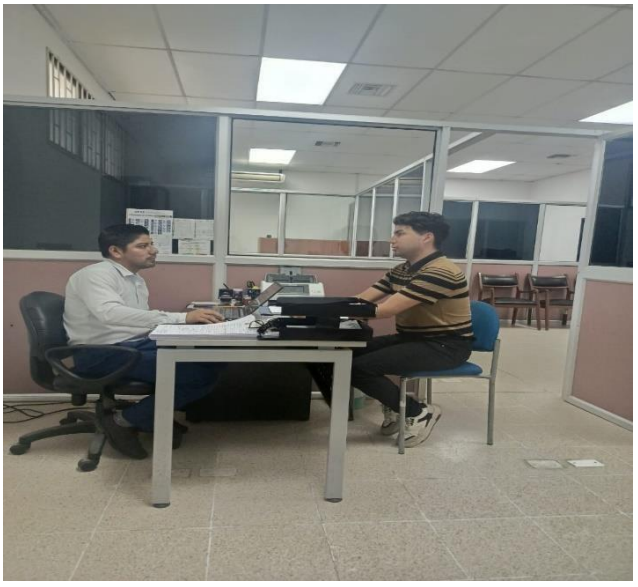


Anexo 4

Entrevistas al personal de talento humano y sistemas del municipio del cantón Salinas

Anexo 3

Entrevistas al personal de talento humano y sistemas de la Universidad Estatal Península de Santa Elena UPSE

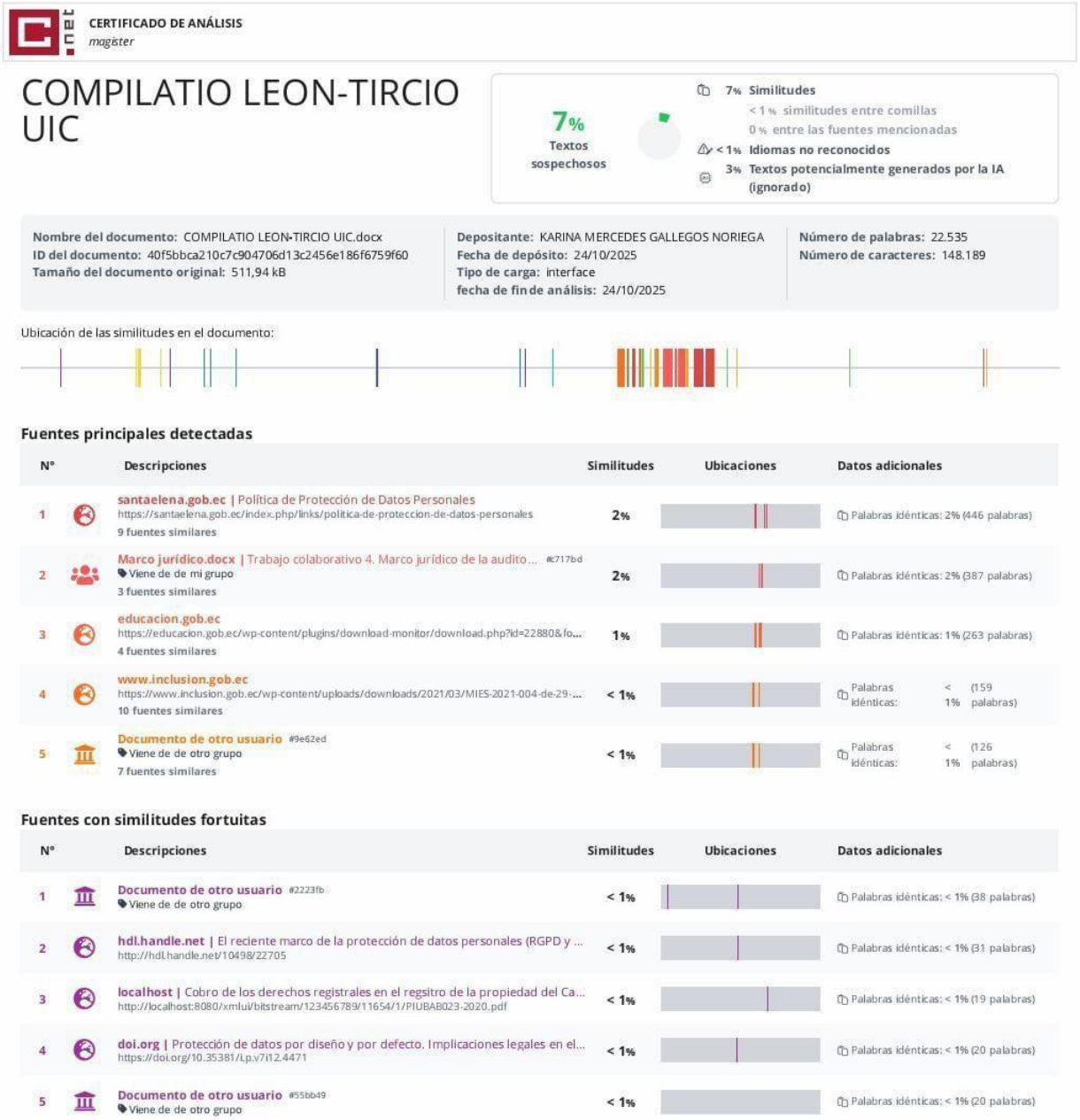


Anexo 5

Tutorías de UIC

Anexo 6

Certificado de análisis de Compilatio remitido por la Tutora Ab. Karina Gallegos



CERTIFICADO DE ANÁLISIS
*magister*

# COMPILATIO LEON-TIRCIO UIC

**7%** Textos sospechosos

- 7% Similitudes
- < 1 % similitudes entre comillas
- 0 % entre las fuentes mencionadas
- < 1% Idiomas no reconocidos
- 3% Textos potencialmente generados por la IA (ignorado)

**Nombre del documento:** COMPILATIO LEON-TIRCIO UIC.docx
**ID del documento:** 40f5bbca210c7c904706d13c2456e186f6759f60
**Tamaño del documento original:** 511,94 kB

**Depositante:** KARINA MERCEDES GALLEGOS NORIEGA
**Fecha de depósito:** 24/10/2025
**Tipo de carga:** interface
**fecha de fin de análisis:** 24/10/2025

**Número de palabras:** 22.535
**Número de caracteres:** 148.189

Ubicación de las similitudes en el documento:

## Fuentes principales detectadas

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | santaelena.gob.ec \| Política de Protección de Datos Personales<br>https://santaelena.gob.ec/index.php/links/politica-de-proteccion-de-datos-personales<br>9 fuentes similares | 2% | | Palabras idénticas: 2% (446 palabras) |
| 2 | Marco jurídico.docx \| Trabajo colaborativo 4. Marco jurídico de la audito... #c717bd<br>Viene de de mi grupo<br>3 fuentes similares | 2% | | Palabras idénticas: 2% (387 palabras) |
| 3 | educacion.gob.ec<br>https://educacion.gob.ec/wp-content/plugins/download-monitor/download.php?id=22880&fo...<br>4 fuentes similares | 1% | | Palabras idénticas: 1% (263 palabras) |
| 4 | www.inclusion.gob.ec<br>https://www.inclusion.gob.ec/wp-content/uploads/downloads/2021/03/MIES-2021-004-de-29-...<br>10 fuentes similares | < 1% | | Palabras idénticas: < 1% (159 palabras) |
| 5 | Documento de otro usuario #9e62ed<br>Viene de de otro grupo<br>7 fuentes similares | < 1% | | Palabras idénticas: < 1% (126 palabras) |

## Fuentes con similitudes fortuitas

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | Documento de otro usuario #2223fb<br>Viene de de otro grupo | < 1% | | Palabras idénticas: < 1% (38 palabras) |
| 2 | hdl.handle.net \| El reciente marco de la protección de datos personales (RGPD y ...<br>http://hdl.handle.net/10498/22705 | < 1% | | Palabras idénticas: < 1% (31 palabras) |
| 3 | localhost \| Cobro de los derechos registrales en el regsitro de la propiedad del Ca...<br>http://localhost:8080/xmlui/bitstream/123456789/11654/1/PIUBAB023-2020.pdf | < 1% | | Palabras idénticas: < 1% (19 palabras) |
| 4 | doi.org \| Protección de datos por diseño y por defecto. Implicaciones legales en el...<br>https://doi.org/10.35381/i.p.v7i12.4471 | < 1% | | Palabras idénticas: < 1% (20 palabras) |
| 5 | Documento de otro usuario #55bb49<br>Viene de de otro grupo | < 1% | | Palabras idénticas: < 1% (20 palabras) |