



**UPSE**

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**TÍTULO DEL TRABAJO DE TITULACIÓN  
POLÍTICAS INTERNAS Y TRATAMIENTO DE DATOS  
PERSONALES DEL CUERPO DE BOMBEROS MUNICIPAL  
DE MACHALA, 2025**

**AUTOR**

Ing. Ochoa Padilla Elías Wilfrido

**TRABAJO DE TITULACIÓN EN MODALIDAD DE  
INFORME DE INVESTIGACIÓN  
Previo a la obtención del grado académico en  
MAGÍSTER EN ADMINISTRACIÓN PÚBLICA**

**TUTORA**

PhD. Sabando Mendoza Estela Rossana

**La Libertad, Ecuador**

**2026**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**TRIBUNAL DE SUSTENTACIÓN**

---

**PhD. Homero Rodríguez Insuasti  
COORDINADOR DEL PROGRAMA**

---

**PhD. Estela Sabando Mendoza  
TUTORA**

---

**PhD. Luis Torres Barrera  
DOCENTE ESPECIALISTA**

---

**PhD. Edgar Cañizares Cedeño  
DOCENTE ESPECIALISTA**

---

**Ab. María Rivera González, Mgtr.  
SECRETARIA GENERAL  
UPSE**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**CERTIFICACIÓN**

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por ELÍAS WILFRIDO OCHOA PADILLA, como requerimiento para la obtención del título de Magíster en Administración Pública.

**TUTORA**

---

**PhD. Estela Sabando Mendoza**

**28 días del mes de abril del año 2026**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**DECLARACIÓN DE RESPONSABILIDAD**

**Yo, ELÍAS WILFRIDO OCHOA PADILLA**

**DECLARO QUE:**

El trabajo de Titulación, (Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025) previo a la obtención del título en Magíster en Administración Pública, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 28 días del mes de abril del año 2026

**EL AUTOR**

---

**Ochoa Padilla Elías Wilfrido**



**UPSE**

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**CERTIFICACIÓN DE ANTIPLAGIO**

Certifico que después de revisar el documento final del trabajo de titulación denominado Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025, presentado por el estudiante, ELÍAS WILFRIDO OCHOA PADILLA fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis  
Compilatio Magister+ | UPSE-ECU

DOC INFORME DE INVESTIGACIÓN (1)

ID : 5966f1483441c39465a2ff83d3eff656bff4ee40



**9%**  
Textos sospechosos

Nombre del fichero : DOC INFORME DE INVESTIGACIÓN (1).txt  
Tamaño del archivo original : 1,39 MB  
Número de palabras : 11.121  
Número de caracteres : 77440

Depositante : ESTELA ROSSANA SABANDO MENDOZA  
Fecha de depósito : 27 de abril de 2026  
Tipo de carga : interface  
fecha de fin de análisis : 27 de abril de 2026

**TUTORA**

---

**PhD. Estela Sabando Mendoza**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS ADMINISTRATIVAS  
INSTITUTO DE POSTGRADO**

**AUTORIZACIÓN**

**Yo, ELÍAS WILFRIDO OCHOA PADILLA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de informe de investigación con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

La Libertad, a los 28 días del mes de abril del año 2026

**EL AUTOR**

---

**Ochoa Padilla Elías Wilfrido**

## AGRADECIMIENTO

A la Universidad Estatal Península de Santa Elena y a su Instituto de Postgrado, por brindarme la oportunidad de alcanzar esta meta académica y por permitirme desarrollar mis conocimientos en la administración de la gestión pública.

Un agradecimiento especial a mi tutora, la Ing. Rossana Sabando Mendoza, PhD., cuya guía, paciencia y valiosas orientaciones fueron fundamentales para la estructura final de esta investigación.

De igual manera, expreso mi gratitud a los funcionarios del Cuerpo de Bomberos Municipal de Machala, quienes permitieron el acceso a la información necesaria para el diagnóstico institucional, para poder mapear los procedimientos y poder implementar una mejora continua y la protección de los derechos de la ciudadanía

*Elías Wilfrido, Ochoa Padilla*

## **DEDICATORIA**

Dedico este logro primordialmente a Dios, por ser mi guía y fortaleza en cada paso de este camino profesional y personal.

A mi amada esposa Pamela, por su apoyo incondicional y por ser el pilar fundamental que me motiva a superarme cada día. A mi hija Ema, quien es mi mayor fuente de inspiración diaria; espero que este esfuerzo le sirva de ejemplo sobre la importancia de la perseverancia y la educación.

A mis padres amados Doris y Antonio, por haberme inculcado los valores de responsabilidad y perseverancia, al no rendirme, con los obstáculos que la vida presenta, que hoy aplico en mi vida profesional dentro de la administración pública. Este título es también de ustedes.

*Elías Wilfrido, Ochoa Padilla*

# ÍNDICE GENERAL

TÍTULO DEL TRABAJO DE TITULACIÓN .....	I
TRIBUNAL DE SUSTENTACIÓN .....	II
CERTIFICACIÓN.....	III
DECLARACIÓN DE RESPONSABILIDAD .....	IV
DECLARO QUE: .....	IV
CERTIFICACIÓN DE ANTIPLAGIO .....	V
AUTORIZACIÓN .....	VI
AGRADECIMIENTO .....	VII
DEDICATORIA.....	VIII
ÍNDICE GENERAL .....	IX
ÍNDICE DE TABLAS .....	XI
ÍNDICE DE FIGURAS .....	XII
RESUMEN .....	XIII
ABSTRACT.....	XIV
INTRODUCCIÓN .....	1
<b>CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL.....</b>	<b>5</b>
1.1. Revisión de literatura .....	5
1.2. Desarrollo teórico y conceptual .....	7
1.2.1. Políticas internas y su utilidad organizacional.....	8
1.2.2. Teoría Institucional y el Isomorfismo Normativo .....	8
1.2.3. Teoría de la Contingencia en la Gestión de Información .....	8
1.2.4. Principios del Tratamiento de Datos.....	9
1.2.5. Definiciones Críticas y Ciclo de Vida del Dato Institucional.....	10
1.2.6. Marco Normativo y el tratamiento de datos en Ecuador .....	10

1.2.7. Marco Normativo de bomberos y reglamentación Municipal .....	11
<b>CAPÍTULO 2. METODOLOGÍA.....</b>	<b>12</b>
2.1. Contexto de la investigación .....	12
2.2. Diseño y alcance de la investigación .....	12
2.3. Tipo y métodos de investigación.....	12
2.4. Población y muestra .....	13
2.5. Técnicas e instrumentos de recolección de datos.....	13
2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información. ....	14
<b>CAPÍTULO 3. RESULTADOS Y DISCUSIÓN .....</b>	<b>15</b>
3.1. Presentación de Resultados según Objetivos Específicos.....	15
3.1.1. Fundamentación teórica y bibliográfica de políticas internas y principios del tratamiento de datos personales .....	15
3.1.2. Diagnóstico del estado actual de procesos de manejo de información y cumplimiento de la LOPDP .....	16
3.1.3. Diseño de políticas internas de tratamiento de datos personales .....	20
3.1.4. Validación de la propuesta mediante juicio de expertos.....	25
3.2. Discusión de Resultados .....	27
3.3. Contratación de la Hipótesis.....	29
<b>CONCLUSIONES .....</b>	<b>30</b>
<b>RECOMENDACIONES .....</b>	<b>33</b>
<b>REFERENCIAS.....</b>	<b>35</b>
<b>ANEXOS.....</b>	<b>39</b>

## ÍNDICE DE TABLAS

<b>Tabla 1</b> <i>Distribución de la población del Cuerpo de Bomberos Municipal de Machala</i> .....	13
<b>Tabla 2</b> <i>Resultados de la encuesta: Variable Políticas Internas (V1)</i> .....	16
<b>Tabla 3</b> <i>Resultados de la encuesta: Variable Tratamiento de Datos Personales (V2)</i> ..	17
<b>Tabla 4</b> <i>Plazos de conservación</i> .....	23
<b>Tabla 5</b> <i>Resultados de validación por juicio de expertos</i> .....	26

## ÍNDICE DE FIGURAS

<b>Figura 1</b>	<i>Modelo integrador de gestión de datos personales para el CBM-M.....</i>	<i>7</i>
-----------------	--	----------

## RESUMEN

Proteger los datos personales es un reto importante para la administración pública de Ecuador, especialmente para los primeros en responder como el Departamento Municipal de Bomberos de Machala (CBM-M), donde la necesidad de acción rápida a menudo conduce a un manejo menos cuidadoso de información sensible. El presente trabajo de investigación pretende crear una propuesta de políticas internas sobre cómo manejar los datos personales en la CBM-M en 2025, con el objetivo de mejorar la gestión administrativa y garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP). Se utilizó una metodología descriptiva mixta con un diseño no experimental, aplicando encuestas censales a 200 funcionarios y entrevistas semiestructuradas a 5 directores. Los resultados revelaron un problema importante: el 80% del personal no tiene formación en LOPDP, el 75% desconoce los protocolos de notificación de incidentes y el 78% pasa por alto los procedimientos de eliminación segura, junto con la falta de un Delegado de Protección de Datos y políticas institucionales oficiales. Sobre la base del diagnóstico, se creó una propuesta de reglamentación de diez títulos que reúne principios rectores, gobernanza de los datos, protocolos operativos de emergencia, medidas técnicas y organizativas de seguridad, derechos de los titulares, ciclo de vida de la información y auditorías. Se concluye que la creación de políticas internas específicas es esencial para pasar de la gestión informal a un estándar de protección de datos que equilibre la agilidad operativa de los bomberos con el respeto de los derechos fundamentales de los ciudadanos.

**Palabras claves:** Protección de datos personales, Políticas institucionales, Administración Pública

## ABSTRACT

Protecting personal data is a significant challenge for Ecuador's public administration, especially for first responders such as the Machala Municipal Fire Department (CBM-M), where the need for rapid action often leads to less careful handling of sensitive information. This research work aims to create a proposal for internal policies on how to handle personal data at the CBM-M in 2025, with the objective of improving administrative management and ensuring compliance with the Organic Law on Personal Data Protection (LOPDP). A mixed descriptive methodology with a non-experimental design was used, applying census surveys to 200 officials and semi-structured interviews to 5 directors. The results revealed a significant problem: 80% of the staff have no training in the LOPDP, 75% are unaware of incident notification protocols, and 78% overlook secure disposal procedures, along with the lack of a Data Protection Officer and official institutional policies. Based on the diagnosis, a ten-title regulatory proposal was created, bringing together guiding principles, data governance, emergency operational protocols, technical and organizational security measures, rights of data subjects, the information life cycle, and audits. It is concluded that the creation of specific internal policies is essential to transition from informal management to a data protection standard that balances the operational agility of firefighters with respect for the fundamental rights of citizens.

**Keywords:** Personal data protection, Institutional policies, Public administration.

# INTRODUCCIÓN

La protección de los datos personales constituye en la actualidad uno de los principales desafíos de la administración pública, especialmente en un entorno caracterizado por el uso intensivo de tecnologías, la digitalización de la información y la demanda ciudadana de mayor transparencia y respeto a los derechos fundamentales. Las instituciones públicas, en su calidad de responsables del tratamiento de datos personales, están llamadas no solo a cumplir con el marco jurídico vigente, sino también a desarrollar políticas internas que orienten de manera clara, uniforme y segura la gestión de la información que administran.

En mayo de 2021, Ecuador dio un paso al aprobar la Ley Orgánica de Protección de Datos Personales para salvaguardar la dignidad y la intimidad de los ciudadanos en la era digital (LOPDP, 2021). Sin embargo, llevar la ley a la práctica cotidiana resulta más complejo de lo que parece, especialmente en donde la urgencia y el servicio operativo son el pan de cada día, como es el caso de los cuerpos de bomberos. Por ello, es importante que en estas entidades el manejo de la información personal merezca cuidado y respeto.

Imaginar una escena donde una persona realiza una llamada de emergencia alertando sobre un incendio, los bomberos llegan al lugar y atienden a las víctimas, a su vez registran sus nombres, estados de salud y direcciones exactas. Esta información que ha sido recolectada en medio del caos y la urgencia, es altamente sensible. ¿Qué ocurre con esos datos después? ¿Quién garantiza que no terminen en manos equivocadas? ¿Existe alguien responsable de proteger la privacidad de quienes ya están pasando por una situación vulnerable? En el Cuerpo de Bomberos Municipal de Machala (CBM-M), como en muchas instituciones similares, estas preguntas no cuentan con respuestas claras.

El CBM-M es una entidad pública que se encarga de la atención de emergencias, prevención de riesgos y protección de la ciudadanía, además gestiona de manera permanente datos personales de ciudadanos, víctimas de siniestros, personal operativo, administrativo y voluntario, y durante más de dos años de vigencia de la ley, esta institución ha continuado operando sin políticas claras que orienten cómo debe manejarse los datos una vez que la emergencia termina. La falta de políticas internas

claras y protocolos estandarizados otorga un riesgo legal para la institución, además de debilitar la confianza que la ciudadanía deposita en medio de una emergencia.

Frente a esta situación, surge la siguiente pregunta de investigación: ¿cómo se puede desarrollar políticas internas que permitan al CBM-M cumplir con la ley sin arriesgar la rapidez que exige su labor? Por ello, esta investigación tiene como objetivo principal desarrollar políticas internas para el tratamiento de datos personales en el CBM-M durante el año 2025, con el propósito de fortalecer la gestión administrativa y asegurar el cumplimiento de la LOPDP; mientras que el alcance del estudio aborda específicamente cómo fortalecer la gestión administrativa desde una perspectiva de administración pública, examinando qué dice la normativa vigente, cómo se maneja realmente la información y qué mecanismos de control faltan.

A fin de lograr un diagnóstico real, este trabajo emplea una investigación profunda de las prácticas actuales del tratamiento de datos en la institución, analiza los marcos normativos y teóricos que guían la propuesta y diseño de las políticas internas. El enfoque metodológico es mixto dado que combina el análisis documental y normas con técnicas de entrevistas y encuestas al personal operativo y administrativo, a fin de comprender la magnitud del problema y las razones que lo sustentan.

La importancia de esta investigación, desde el ámbito social, contribuye a garantizar los derechos de la ciudadanía cuando atraviesan momentos difíciles; en lo profesional, fortalece la estructura interna del CBM-M mediante herramientas concretas para mejorar la gestión de la entidad; y en lo académico, aporta a la protección de datos para que otras instituciones tomen como referencia la propuesta elaborada y se multiplique su impacto. En definitiva, el presente trabajo busca la ética en la gestión pública y el respeto absoluto a la privacidad.

Finalmente, el trabajo se organiza en tres capítulos. El capítulo 1 desarrolla las bases teóricas y normativas que sustentan la protección de datos. El capítulo 2 detalla la metodología empleada en la investigación y el levantamiento de la información. El capítulo 3 presenta los resultados obtenidos, su análisis y discusión, a partir de los cuales se formulan las conclusiones y recomendaciones orientadas al fortalecimiento de la gestión pública institucional.

## **Planteamiento de la investigación**

En el ámbito internacional, las políticas internas de las instituciones se constituyen por un conjunto de normas, directrices y procedimientos que orientan el funcionamiento de las organizaciones, especialmente en entidades públicas. Estas políticas son una brújula que orienta al comportamiento organizacional a fin de garantizar transparencia y eficiencia en los procesos administrativos. (Torres-Baque, J. R., & Pibaque-Pionce, M. S., 2024). Sin embargo, a nivel nacional existe una realidad compleja, mientras que la LOPDP exige principios de lealtad, transparencia y responsabilidad proactiva en el tratamiento de datos personales, muchas entidades aún no logran implementar estas exigencias a su operatividad diaria.

Esta brecha significativa entre lo que indica la ley y lo que sucede en la práctica es alarmante en sectores estratégicos como los cuerpos de bomberos, puesto que se maneja información extremadamente sensible de víctimas de siniestros, pacientes y del personal de primera respuesta. La ausencia de protocolos claros pone en riesgo los derechos fundamentales de los ciudadanos, quienes en momentos vulnerables ponen su confianza en terceras personas. (Ciudadanía y Desarrollo, 2021).

De manera particular para esta institución, CBM-M, la situación se vuelve crítica. Durante un levantamiento de información inicial realizado los días 21 y 22 de mayo del 2025 mediante la aplicación de una entrevista al personal operativo y administrativo, y se pudo constatar que, a pesar de estar sujetos a la LOPDP, el personal opera sin una guía institucional estandarizada. La ausencia de políticas internas ocasiona una gestión de datos débil, lo cual no solo afecta la transparencia administrativa, sino que desgasta la confianza de la ciudadanía machaleña.

En la dinámica diaria, el personal administrativo y operativo ha manifestado la preocupación de no estar capacitados para el adecuado manejo de datos personales, surgiendo prácticas informales, almacenamiento inseguro y falta de consentimiento informado. Esta informalidad puede causar filtraciones de datos, mal uso de información privada, y eventualmente, sanciones legales que podrían comprometer a la institución.

## **Formulación del problema de investigación**

Bajo este contexto, surge la siguiente interrogante: ¿Por qué el personal operativo y administrativo del Cuerpo de Bomberos Municipal de Machala no emplea prácticas estandarizadas y seguras en el tratamiento de datos personales, a pesar de las exigencias del marco legal vigente en el Ecuador?

## **Objetivo General:**

Desarrollar una propuesta de políticas internas para el tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala durante el año 2025.

## **Objetivos Específicos:**

1. Fundamentar teórica y bibliográficamente las políticas internas y los principios del tratamiento de datos personales en la administración pública.
2. Diagnosticar el estado actual de los procesos de manejo de información y el nivel de cumplimiento de la LOPDP en la institución.
3. Diseñar las políticas internas de tratamiento de datos personales alineadas a la normativa legal vigente.

## **Planteamiento hipotético**

Idea a Defender: La investigación parte de la actualidad vulnerabilidad en el manejo de la información dentro del Cuerpo de Bomberos Municipal de Machala; en este sentido, se sostiene que la ausencia de políticas institucionales claras y de protocolos estandarizados, incide negativamente en la gestión institucional, el control interno y la garantía del derecho a la protección de datos personales. Por lo tanto, el diseño, elaboración y propuesta de dichas políticas permitirá fortalecer la gestión pública y asegurar el cumplimiento efectivo y ético de la Ley Orgánica de Protección de Datos Personales.

# CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

## 1.1. Revisión de literatura

La literatura académica reciente sobre la protección de datos personales subraya una transición necesaria desde el cumplimiento formal hacia una gestión operativa eficiente, especialmente en entidades de respuesta a emergencias. A continuación, se presenta un análisis comparativo de estudios desarrollados en los últimos cinco años que fundamentan la necesidad de fortalecer las políticas internas en instituciones públicas.

Desde la perspectiva internacional, Badillo (2021), en su artículo científico titulado “COVID-19 y protección de datos personales”, planteó como objetivo principal el análisis del tratamiento de información sensible por parte de organismos de socorro en contextos de crisis sanitaria. La metodología que aplicó fue de tipo cualitativa con un diseño documental-bibliográfico, que se fundamentaba en el análisis de contenido de normativas europeas. El procesamiento de datos lo realizó mediante la técnica de triangulación normativa, comparando los estándares del RGPD con las prácticas institucionales. Como principal conclusión, mantiene que el tratamiento de datos en situaciones de emergencia exige utilizar protocolos de seguridad reforzados y aplicar una limitación estricta de los datos para evitar que la eficiencia operativa trasgreda la privacidad de la ciudadanía.

Por otra parte, Pardo Luna y Abarca Cruz (2025), en su artículo científico titulado "Aplicación de la ley orgánica de datos personales en entidades públicas; aspectos a la protección del derecho a la intimidad", plantearon como objetivo general, identificar las vulnerabilidades críticas en el manejo de datos personales por parte de entidades públicas ecuatorianas bajo la LOPDP. La metodología aplicada en este trabajo fue cualitativa con alcance exploratorio-descriptivo, para lo cual se empleó el método de análisis de contenido de normativa legal y jurisprudencia nacional. Para el procesamiento de datos, realizó la técnica de categorización temática de disposiciones legales, permitiendo obtener como principal conclusión que la ausencia de políticas de ciberseguridad y de control de acceso jerárquico en las instituciones públicas aumenta la probabilidad de incidentes de seguridad que comprometen la integridad de los ciudadanos y vulneran su derecho fundamental a la intimidad.

En el plano local, Ochoa, N. V. V., Álvarez, M. Á. M., y Manzano, R. L. M. (2024), en su tesis de maestría titulada “Implementación de medidas de seguridad y principio de conservación de datos en instituciones públicas”, lograron evaluar el de cumplimiento de las políticas que salvaguarden la información en entidades gubernamentales latinoamericanas. Esta investigación empleó una metodología mixta con un alcance descriptivo, utilizando la encuesta como técnica primordial. Para el procesamiento de datos, se ejecutó a través de estadística descriptiva mediante el software SPSS, el cual permitió cuantificar las brechas de seguridad. Su principal conclusión fue que la mayoría de las instituciones carecen de inventarios de activos de información y de políticas de eliminación segura, lo que genera un riesgo crítico de filtración de datos personales por incumplimiento a la normativa.

Conforme a la Superintendencia de Protección de Datos Personales (2025), en su documento técnico "Plan Nacional de Protección de Datos Personales 2025", buscó establecer un marco estratégico para el manejo de la información y la privacidad en el sector público ecuatoriano. El documento empleó una metodología de investigación normativa y análisis de brechas institucionales, aplicando cuestionarios y talleres participativos con funcionarios de nivel directivo de diversas entidades públicas. La recolección de la información se llevó a cabo mediante análisis de contenido para identificar factores de resistencia al cambio organizacional y necesidades de fortalecimiento institucional, obteniendo como principal conclusión que la gobernanza de datos en instituciones públicas falla debido a la carencia de un Oficial de Protección de Datos (DPD) designado formalmente y a la inexistencia de protocolos internos que definan las responsabilidades de cada área en la cadena de custodia de la información personal.

Finalmente, en el Ecuador, Jaramillo (2025), en su artículo científico titulado “Análisis comparado sobre la protección de datos personales en el Ecuador”, planteó como objetivo central diagnosticar el estado de implementación de la LOPDP en los Gobiernos Autónomos Descentralizados y sus entidades adscritas; y una metodología analítico-deductivo con enfoque cualitativo-jurídico, revisando la estructura de las ordenanzas municipales frente a la ley nacional. Para el procesamiento de datos se basó en el análisis de matrices de cumplimiento normativo, concluyendo principalmente que existe una brecha significativa en el principio de responsabilidad proactiva, debido a que las instituciones mantienen reglamentos internos desactualizados que no contemplan las

nuevas obligaciones de seguridad y notificación de vulneraciones exigidas por la autoridad de control ecuatoriana.

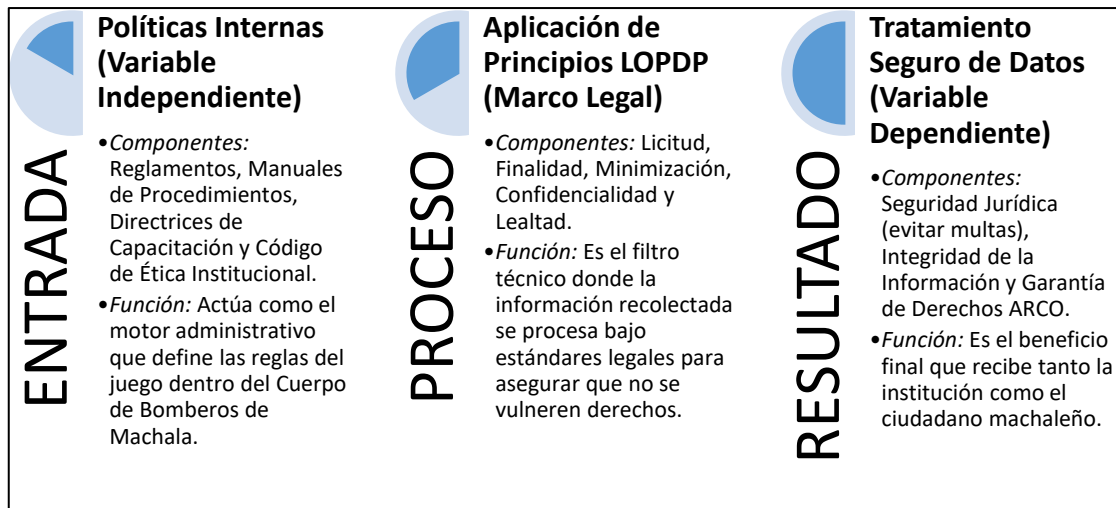
Mientras tanto, Vera, Ortega y Preciado (2024), en su artículo científico titulado "Propuesta de Gobierno Electrónico para Mejorar el Proceso de Gestión Documental en el Municipio de Babahoyo 2023", muestra como objetivo general el analizar la adaptación de los procesos de archivo y digitalización a las nuevas exigencias de protección de datos en entidades municipales. Para este trabajo se aplicó una metodología con enfoque mixto con un diseño de investigación-acción, aplicando entrevistas y auditorías documentales en el área de estadística; mientras que para el procesamiento de datos se realizó un análisis de procesos y flujogramas para la codificación de categorías de gestión documental. La conclusión principal resalta que las entidades adscritas a los municipios, incluyendo servicios de emergencia, presentan un atraso en la implementación de cláusulas de confidencialidad en sus contratos y formularios, lo que genera una exposición jurídica ante posibles auditorías de las autoridades de control en materia de protección de datos personales.

## **1.2. Desarrollo teórico y conceptual**

El tratamiento de datos personales en una entidad de primera respuesta no solo es un desafío técnico, sino un fenómeno organizacional que puede ser comprendido a través de diversas corrientes del pensamiento administrativo y jurídico. Para la presente investigación, se han seleccionado teorías que permiten explicar por qué el Cuerpo de Bomberos Municipal de Machala requiere una estructura interna formal para la protección de la información.

### **Figura 1**

*Modelo integrador de gestión de datos personales para el CBM-M*



### 1.2.1. Políticas internas y su utilidad organizacional

Las políticas internas se definen como directrices que dictan el comportamiento de los funcionarios para asegurar que la entidad opere bajo principios de transparencia, coherencia y eficiencia. (Pazmiño, 2023). Según el Ministerio de Trabajo y Seguridad Social (2022), la importancia de estos lineamientos radica en su capacidad para formalizar procesos que antes eran empíricos en normas explícitas que orienta la toma de decisiones. Al convertir las prácticas cotidianas en normas escritas, se facilita la rendición de cuentas y se asegura que cada proceso administrativo sea auditable y transparente. (García-Falconí, 2022).

### 1.2.2. Teoría Institucional y el Isomorfismo Normativo

Desde la perspectiva de la Teoría Institucional, DiMaggio y Powell (1983) sostienen que las organizaciones tienden a adoptar estructuras y procesos no solo por eficiencia, sino por la necesidad de alcanzar legitimidad dentro de su entorno. Para el CBM-M la implementación de estas normativas responde a una presión externa debido a la obligación a cambiar sus procesos para cumplir con la LOPDP a fin de evitar multas o procesos legales de una gestión de datos deficiente. (OEA, 2021).

### 1.2.3. Teoría de la Contingencia en la Gestión de Información

Según Fiedler (1964), la Teoría de la Contingencia señala que existe más de una forma para organizar una institución puesto que depende de la tecnología y el entorno. Para el caso del CBM-M que se enfrentan a un escenario de alta volatilidad, donde la gestión de información sensible sucede en intervalos de tiempos mínimos y bajo una presión extrema (Superintendencia de Protección de Datos Personales del Ecuador, 2025); esta

realidad justifica que el tratamiento de datos personales no puede limitarse a la adopción de manuales administrativos estáticos, sino por protocolos diseñados bajo un enfoque de contingencia que garantice la confidencialidad y la integridad de la información sensible de los ciudadanos, sin comprometer la agilidad y la inmediatez que exige el servicio de auxilio.

#### **1.2.4. Principios del Tratamiento de Datos**

Desde mayo de 2021, la LOPDP ha reconfigurado la forma en que el estado ecuatoriano gestiona la información ciudadana. Esta normativa establece un marco ético que obliga a las instituciones, sea pública o privada, a garantizar que la privacidad sea el centro de sus operaciones y se respete los derechos de la ciudadanía respecto al tratamiento adecuado de sus datos personales. (Asamblea Nacional del Ecuador, 2021).

En la práctica, esto se divide en seis pilares fundamentales. El principio de licitud exige que cada dato obtenido cuente con una base legal clara (Echeverría Muñoz, D., 2025); puesto que no se trata de recolectar datos porque la tecnología lo permite, sino que debe justificarse legalmente. Mientras que el principio de finalidad actúa como un límite, dado que la información debe utilizarse exclusivamente para el propósito original, evitando que las bases de datos terminen en bases de datos para fines (Alzate, J. P., 2025).

La eficiencia administrativa sugiere que menos es más, bajo este principio de minimización, las instituciones deben recolectar la información estrictamente necesaria para cumplir su misión, evitando la acumulación de datos irrelevantes que solo aumentan los riesgos institucionales. (Kruger Law, 2025). El principio de transparencia es la base de la confianza ciudadana puesto que garantiza que el titular de los datos tenga pleno conocimiento de quién, cómo y para qué se procesa su información (HLB Ecuador, 2025).

En cuanto al principio de seguridad, la ley exige implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra filtraciones o pérdidas; esto incluye el uso de un software seguro y la cultura del personal que maneja la información sensible cada día. (Asamblea Nacional del Ecuador, 2021). Finalmente, el principio de responsabilidad proactiva traslada la carga de la prueba a la institución; es decir, ya no basta con indicar que se cumple con la normativa, sino que el responsable debe demostrar mediante políticas documentadas, auditorías y evidencias claras de estar aplicando buenas prácticas de gestión de datos. (Asamblea Nacional del Ecuador, 2021).

En conjunto, estos principios son la base para construir una cultura de respeto a la privacidad en el Ecuador, fortaleciendo la confianza de la ciudadanía y las instituciones que lo protegen. (Alzate, 2025).

### **1.2.5. Definiciones Críticas y Ciclo de Vida del Dato Institucional**

Los datos sensibles en el ámbito de las emergencias, que incluyen estados de salud o la geolocalización de las víctimas, requieren una protección reforzada debido a que su tratamiento inadecuado podría comprometer gravemente la dignidad o la seguridad del titular. (Superintendencia de Protección de Datos Personales del Ecuador, 2025).

En el CBM-M el ciclo de vida de la información inicia con la recolección de los datos mediante la recepción de llamadas de emergencias y el llenado del formulario de inspección, para posteriormente continuar con el proceso operativo de respuesta inmediata y finalmente culminar con la fase de archivo seguro o eliminación definitiva (Superintendencia de Protección de Datos Personales del Ecuador, 2025). Esta administración técnica garantiza que los datos personales de la ciudadanía no permanezcan en el sistema más del tiempo justificado, respetando así los plazos legales.

### **1.2.6. Marco Normativo y el tratamiento de datos en Ecuador**

El tratamiento de datos personales se refiere a cualquier operación técnica tanto manual o automatizada, que afecte la información de un individuo, desde su recolección hasta su eliminación (Presidencia de la República del Ecuador, 2023). En el Ecuador, este concepto dejó de ser un tema técnico para convertirse en un mandato constitucional a partir de 2008, año en que se consagró la protección de datos como un derecho fundamental (Asamblea Constituyente, 2008).

Desde el ámbito teórico, este marco se asienta en el modelo del Estado constitucional de derechos y justicia; bajo este paradigma, el ciudadano es el único titular y dueño de su información, lo que obliga a las instituciones a respetar el derecho de cada persona a decidir quién usa su información y para qué fines específicos (Superintendencia de Protección de Datos Personales del Ecuador, 2024).

En la actualidad, la LOPDP impone responsabilidades ineludibles para quienes administran datos. Ya no basta con custodiar la información; es imperativo gestionar el consentimiento, asegurar el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y designar figuras clave como el delegado de protección de

datos (Superintendencia de Protección de Datos Personales del Ecuador, 2025). Incluso en el ámbito digital, la ley ha avanzado hacia el reconocimiento de derechos de vanguardia, como la portabilidad y el derecho al olvido, marcando un antes y un después en la privacidad tecnológica del país (Superintendencia de Protección de Datos Personales del Ecuador, 2025).

### **1.2.7. Marco Normativo de bomberos y reglamentación Municipal**

El tratamiento de datos personales en el CBM-M se encuentra condicionado por la naturaleza de sus funciones de primera respuesta. De acuerdo a la ley, el cuerpo de bomberos debe elaborar partes de emergencia (Art. 31 del Reglamento General a la Ley de Defensa Contra Incendios), los cuales se convierten en depósitos de información extremadamente sensible, incluyendo estados de salud y geolocalización de víctimas. Sin políticas internas de custodia, la institución no solo vulneraría la LOPDP, sino que violaría el principio de reserva de información, exponiéndose a graves repercusiones legales por posibles filtraciones.

A nivel local, la base legal se encuentra en la autonomía que la Constitución (Art. 240) y el COOTAD (Art. 140) otorgan al GAD Municipal de Machala. Esta facultad permite que el CBM-M adecúe sus reglamentos internos para proteger la información de sus usuarios. En la actualidad, se identifica una brecha respecto al Art. 4 de la Ley Orgánica de Optimización y Eficiencia de Trámites, ya que, si bien se impulsa la digitalización en Machala, no se han actualizado con la misma celeridad las disposiciones sobre el ciclo de vida y eliminación segura del dato en el ámbito bomberil. (Cuerpo de Bomberos del Distrito Metropolitano de Quito, 2025).

Finalmente, el Reglamento Orgánico de Gestión Organizacional por Procesos del CBM-M actúa como el eje de la gobernanza interna. Las unidades de TIC y Asesoría Jurídica tienen hoy la obligación legal de establecer protocolos de confidencialidad que no sean vistos como una opción, sino como un eje transversal de la gobernanza interna (Echeverría Muñoz, 2025). Solo mediante la integración de la protección de datos en estos reglamentos, se podrá garantizar que cada bombero, en cada intervención territorial, actúe bajo los estándares de responsabilidad proactiva que exige la ley ecuatoriana.

## **CAPÍTULO 2. METODOLOGÍA**

### **2.1. Contexto de la investigación**

La presente investigación se sitúa en el Cuerpo de Bomberos Municipal de Machala, ubicado en la provincia de El Oro, Ecuador; cuya sede principal se encuentra en las calles Bolívar y Ayacucho, operando a través de diversas estaciones distribuidas estratégicamente en el cantón. El estudio se enfoca específicamente en las áreas administrativas y operativas que tienen bajo su responsabilidad la gestión y custodia de datos personales de la ciudadanía, tales como el Departamento de Prevención de Incendios, la Unidad de Tecnologías de la Información (TIC) y el área de Talento Humano.

### **2.2. Diseño y alcance de la investigación**

El estudio se fundamenta en un diseño no experimental, debido a que no se realiza una manipulación deliberada de las variables, sino que se observa el fenómeno del tratamiento de datos y la gestión de políticas internas en su contexto natural para su posterior análisis. En cuanto al alcance de la investigación, esta es de carácter descriptivo, ya que busca especificar las propiedades y características del manejo de la información dentro de la institución, identificando las brechas actuales frente a la normativa legal vigente (LOPDP).

### **2.3. Tipo y métodos de investigación**

La investigación es de tipo mixto, integrando enfoques cuantitativos para medir el nivel de conocimiento del personal y enfoques cualitativos para analizar la estructura normativa interna. En cuanto a los métodos de investigación, se aplicará el método analítico-sintético, que permitirá descomponer la Ley Orgánica de Protección de Datos Personales en sus principios aplicables para luego sintetizar una propuesta de política interna coherente. Asimismo, se empleará el método deductivo, partiendo de las premisas generales de la administración pública y la seguridad de la información para llegar a conclusiones específicas aplicables al Cuerpo de Bomberos Municipal de Machala.

## 2.4. Población y muestra

La población de estudio está integrada por la totalidad del personal que conforma la estructura orgánica del Cuerpo de Bomberos Municipal de Machala. Para efectos de esta investigación, se ha categorizado a los sujetos de estudio según su rol institucional, considerando que cada grupo mantiene un nivel diferenciado de acceso y responsabilidad en el tratamiento de datos personales, desde la operatividad en emergencias hasta la gestión técnica y legal.

Dado que el universo total es de 200 individuos, se ha optado por realizar un estudio censal. Según la metodología de investigación, un censo es apropiado cuando la población es finita y accesible, permitiendo obtener información de todos los elementos del sistema sin errores de muestreo. Esta decisión metodológica garantiza una visión integral del cumplimiento de la LOPDP en todos los niveles de la institución.

**Tabla 1**

*Distribución de la población del Cuerpo de Bomberos Municipal de Machala*

<b>Categoría de Personal</b>	<b>Número de Personas</b>	<b>Porcentaje (%)</b>
Bomberos operativos	120	60%
Personal administrativo	40	20%
Personal técnico (TI, legal, etc.)	20	10%
Voluntarios	20	10%
<b>Total</b>	<b>200</b>	<b>100%</b>

## 2.5. Técnicas e instrumentos de recolección de datos

Se utilizarán técnicas de carácter mixto para asegurar la triangulación de la información:

- **Técnica Cuantitativa (Encuesta):** Se aplicará un cuestionario estructurado al personal para diagnosticar el nivel de cumplimiento de los principios de seguridad y privacidad.

**Técnica Cualitativa (Entrevista):** Se realizará una entrevista semiestructurada dirigida al Jefe del Departamento Jurídico o al responsable del área de Tecnologías de la Información, con el fin de profundizar en los protocolos técnicos y legales existentes.

## **2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.**

Para garantizar el rigor científico, la validez de los instrumentos se realizará mediante la técnica de Juicio de Expertos, sometiendo el cuestionario y la guía de entrevista a la revisión de tres profesionales con grado de magíster o doctorado en áreas afines. En cuanto a la confiabilidad estadística, se aplicará una prueba piloto al 10% de la población para calcular el coeficiente Alfa de Cronbach. Un resultado superior a 0.80 confirmará que el instrumento es altamente confiable y que sus ítems miden de manera consistente la variable objeto de estudio.

El procesamiento de datos cuantitativos se realizará en el software IBM SPSS Statistics v.27. Se utilizará estadística descriptiva y, para la contratación de la idea a defender (hipótesis), se aplicará la prueba no paramétrica Chi-cuadrado de Pearson ( $X^2$ ). Esta prueba permitirá determinar si existe una relación estadísticamente significativa entre la ausencia de políticas internas y las deficiencias en el tratamiento de datos, considerando un nivel de confianza del 95% y un margen de error del 5%.

Por su parte, el análisis cualitativo se efectuará mediante el software Atlas.ti v.23, empleando el análisis de contenido para la codificación y generación de redes semánticas que permitan interpretar los testimonios de los directivos (vulnerabilidad legal, gobernanza y cultura institucional), facilitando una interpretación profunda de la visión directiva sobre la seguridad de la información.

## **CAPÍTULO 3. RESULTADOS Y DISCUSIÓN**

### **3.1. Presentación de Resultados según Objetivos Específicos**

#### **3.1.1. Fundamentación teórica y bibliográfica de políticas internas y principios del tratamiento de datos personales**

El análisis documental y normativo realizado permite establecer que el manejo confidencial de datos personales, en el ámbito de la administración pública ecuatoriana se fundamenta en un marco constitucional robusto, articulado principalmente con la Constitución de la República del Ecuador en sus artículos 66, numeral 19 y 71 (Asamblea Constituyente, 2008), en donde se reconoce como un derecho fundamental la protección de datos personales. Esto se consolidó en mayo de 2021 con la aprobación de la Ley Orgánica de Protección de Datos Personales (LOPDP), norma que no solo define el derecho, sino que impone obligaciones específicas a las entidades públicas.

Al revisar la literatura especializada, se percibe un esfuerzo global por institucionalizar estas políticas, especialmente en organismos de primera respuesta. Badillo (2021) indica que estas instituciones enfrentan el reto de evitar sacrificar la eficiencia operativa al implementar protocolos de seguridad reforzados. No obstante, la realidad latinoamericana es compleja, y Ochoa, Álvarez y Manzano (2024) señalan que persiste una vulnerabilidad crítica, marcada por la falta de inventarios activos y procesos de eliminación segura, generando riesgos de filtraciones de información.

En Ecuador, la Superintendencia de Protección de Datos Personales (2025) en su plan nacional revela que el manejo de datos en el sector público flaquea por dos razones: la ausencia de un oficial de protección de datos y el vacío de protocolos de custodia. A esto se suma la visión de Jaramillo (2025), quién subraya una brecha significativa en la responsabilidad proactiva, donde los reglamentos internos simplemente no se han actualizado conforme a la ley.

La teoría institucional de DiMaggio y Powell (1983) ofrece una explicación lógica a este fenómeno: las instituciones no solo buscan eficiencia, sino legitimidad. En este sentido, el CBM-M es obligado a estandarizar sus procesos con la normativa de protección de datos de la LOPDP; por ello, adoptar políticas internas deja de ser opcional para convertirse en un requisito de supervivencia institucional. De forma complementaria la

teoría de la contingencia de Fiedler (1964) demuestra que, en un entorno de emergencias, el tratamiento de datos debe ser lo suficientemente ágil para no frenar la operatividad, pero bastante sólido para garantizar la confidencialidad.

Finalmente, cualquier intervención en la institución debe alinearse con los pilares de la Asamblea Nacional del Ecuador (2021): licitud, finalidad, minimización, transparencia, seguridad y responsabilidad proactiva. Estos principios constituyen el eje vertebrador de cualquier política institucional de protección de datos.

### 3.1.2. Diagnóstico del estado actual de procesos de manejo de información y cumplimiento de la LOPDP

#### A. Resultados de la encuesta aplicada al personal (N=200)

La encuesta estructurada aplicada al personal tanto operativo como administrativo del Cuerpo de Bomberos Municipal de Machala, permitió diagnosticar el nivel de conocimiento y aplicación de políticas de protección de datos. Los resultados se presentan según las dimensiones analizadas:

**Tabla 2**

*Resultados de la encuesta: Variable Políticas Internas (VI)*

<b>Indicador</b>	<b>Muy en desacuerdo (1)</b>	<b>En desacuerdo (2)</b>	<b>Indiferente (3)</b>	<b>De acuerdo (4)</b>	<b>Muy de acuerdo (5)</b>	<b>Media</b>	<b>DS</b>
Conocimiento de reglamentos internos	35%	28%	20%	12%	5%	2.24	1.12

<b>Indicador</b>	<b>Muy en desacuerdo (1)</b>	<b>En desacuerdo (2)</b>	<b>Indiferente (3)</b>	<b>De acuerdo (4)</b>	<b>Muy de acuerdo (5)</b>	<b>Media</b>	<b>DS</b>
Difusión de directrices claras	42%	30%	15%	10%	3%	2.02	1.05
Capacitación en LOPDP (último año)	55%	25%	12%	6%	2%	1.75	0.98
Existencia de manuales de procedimientos	38%	32%	18%	9%	3%	2.07	1.08

**Interpretación:** El 63% del personal encuestado desconoce o está en desacuerdo con la existencia de reglamentos internos (media 2.24), mientras que el 80% señala que no ha recibido capacitación en LOPDP durante el último año (media 1.75), finalmente el 70% de los encuestados confirman que la entidad opera sin manuales claros en materia de protección de datos. Estos resultados revelan una debilidad en la estructura normativa de la institución.

### **Tabla 3**

*Resultados de la encuesta: Variable Tratamiento de Datos Personales (V2)*

<b>Indicador</b>	<b>Muy en desacuerdo (1)</b>	<b>En desacuerdo (2)</b>	<b>Indiferente (3)</b>	<b>De acuerdo (4)</b>	<b>Muy de acuerdo (5)</b>	<b>Media</b>	<b>DS</b>
Solicitud de consentimiento informado	25%	35%	22%	12%	6%	2.39	1.15
Uso de datos solo para fines específicos	18%	22%	25%	20%	15%	2.72	1.28
Implementación de medidas de seguridad	15%	20%	30%	22%	13%	2.98	1.22
Reporte inmediato de incidentes	45%	30%	15%	7%	3%	1.93	1.08
Eliminación segura de datos	50%	28%	12%	7%	3%	1.85	1.12

**Interpretación:** Aunque existe un mayor nivel de autopercepción en el cumplimiento del principio de finalidad (media 2.72) y medidas de seguridad básicas (media 2.98),

persisten debilidades críticas. El 75% del personal no reporta incidentes de seguridad (media 1.93) y el 78% no conoce protocolos de eliminación segura (media 1.85). Esto sugiere prácticas informales y falta de cultura de reporte.

### *B. Resultados de la entrevista semiestructurada*

Se realizaron entrevistas a 5 directivos clave: Jefe de TIC, Asesor Jurídico, Jefe de Operaciones, Jefe de Prevención y Director Administrativo. El análisis de contenido mediante Atlas.ti v.23 generó las siguientes categorías temáticas:

#### **Categoría 1: Institucionalización normativa**

- No contamos con una política formal de protección de datos. Lo que existe son disposiciones dispersas en el reglamento orgánico, pero nada específico sobre LOPDP (*Asesor Jurídico*).
- El Cuerpo de Bomberos funciona con normas de hace más de 10 años, no se han actualizado para incluir la protección de datos personales (*Director Administrativo*).

#### **Categoría 2: Estructura de gobernanza**

- No existe un Oficial de Protección de Datos designado. Las funciones están repartidas entre TIC y el área legal, pero sin una responsabilidad clara (Jefe de TIC).
- La cadena de custodia de la información no está definida. Cada área maneja sus archivos como considera conveniente (Jefe de Operaciones).

#### **Categoría 3: Seguridad técnica**

- Los equipos no tienen cifrado de disco. Las contraseñas son compartidas en algunos casos, y no existe un sistema de gestión de accesos (Jefe de TIC).
- Los partes de emergencia se archivan en papel y digital, pero sin protocolos de seguridad definidos para ninguno de los dos formatos (Jefe de Prevención).

#### **Categoría 4: Ciclo de vida del dato**

- No hay un inventario de datos ni políticas de retención. La información se acumula sin criterios de eliminación (Asesor Jurídico).

- Desconocemos los plazos legales de conservación para datos de emergencias. Se guarda todo por precaución, indefinidamente (Director Administrativo).

### **3.1.3. Diseño de políticas internas de tratamiento de datos personales**

Con base en el diagnóstico realizado y el marco normativo vigente, se diseña la siguiente propuesta de políticas internas:

*PROPUESTA: POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES DEL CUERPO DE BOMBEROS MUNICIPAL DE MACHALA*

#### **3.1.3.1. Marco normativo de la propuesta**

La propuesta se fundamenta en:

- Constitución de la República del Ecuador (2008), arts. 66.19, 71
- Ley Orgánica de Protección de Datos Personales (2021)
- Reglamento General a la Ley de Defensa Contra Incendios
- COOTAD, art. 140
- Plan Nacional de Protección de Datos Personales 2025 (SPDP)

#### **3.1.3.2. Estructura de la política propuesta**

##### **TÍTULO I: DISPOSICIONES GENERALES**

*Art. 1.- Objeto* Establecer los lineamientos institucionales para el tratamiento de datos personales en el Cuerpo de Bomberos Municipal de Machala, garantizando el cumplimiento de la LOPDP y la protección de los derechos fundamentales de los titulares.

*Art. 2.- Ámbito de aplicación* Aplica a todo el personal (operativo, administrativo, técnico y voluntarios), contratistas, proveedores y terceros que accedan a datos personales en virtud de sus funciones o relaciones con la institución.

*Art. 3.- Definiciones* Se adoptan las definiciones establecidas en el art. 3 de la LOPDP, incorporando específicamente:

- **Datos sensibles en contexto de emergencias:** información sobre estado de salud, geolocalización precisa, datos biométricos y cualquier información que pueda comprometer la seguridad o dignidad de víctimas o personal.

- **Parte de emergencia:** documento oficial que registra datos de incidentes, víctimas y acciones tomadas durante la atención.

## **TÍTULO II: PRINCIPIOS RECTORES**

*Art. 4.- Principios aplicables* Todo tratamiento de datos en la institución se regirá por los principios de:

1. **Licitud:** tratamiento fundado en mandato legal (art. 9 LOPDP) o consentimiento del titular
2. **Finalidad:** uso exclusivo para fines de atención de emergencias, prevención de riesgos, gestión administrativa o estadísticas oficiales
3. **Minimización:** recolección proporcional y limitada a lo necesario
4. **Transparencia:** información clara a los titulares sobre el tratamiento
5. **Seguridad:** medidas técnicas y organizativas apropiadas al nivel de riesgo
6. **Responsabilidad proactiva:** demostración documental del cumplimiento

## **TÍTULO III: GOBERNANZA DE DATOS**

*Art. 5.- Delegado de Protección de Datos (DPD)* Se designa formalmente al Asesor Jurídico como Delegado de Protección de Datos, con las siguientes funciones:

- Supervisar el cumplimiento de la LOPDP y esta política
- Atender consultas y reclamos de titulares
- Cooperar con la autoridad de control
- Informar sobre obligaciones de protección de datos

*Art. 6.- Comité de Protección de Datos* Se crea un comité integrado por: DPD, Jefe de TIC, Jefe de Operaciones, Jefe de Prevención y Director Administrativo, con funciones de coordinación, seguimiento y mejora continua.

*Art. 7.- Responsables y encargados* Se establecen responsabilidades diferenciadas:

- **Responsables del tratamiento:** Dirección General (datos institucionales), Jefes de área (datos de su competencia)
- **Encargados del tratamiento:** personal operativo y administrativo que ejecuta el tratamiento bajo instrucción de los responsables

## **TÍTULO IV: TRATAMIENTO EN OPERACIONES DE EMERGENCIA**

*Art. 8.- Fundamento legal específico* El tratamiento de datos en emergencias se fundamenta en el art. 9, numeral 3 de la LOPDP (interés público esencial) y el mandato constitucional de protección de la vida.

*Art. 9.- Protocolo de recolección* En atención de emergencias se debe:

1. Informar al titular o representante sobre la finalidad del tratamiento, salvo imposibilidad por estado de salud o urgencia
2. Registrar únicamente datos estrictamente necesarios para la atención
3. Documentar en el parte de emergencia la justificación del tratamiento

*Art. 10.- Datos sensibles* El tratamiento de datos sobre estado de salud, discapacidad o condiciones vulnerables requiere:

- Protección reforzada con acceso limitado
- Registro separado de datos de identificación cuando sea posible
- Plazos de conservación reducidos una vez finalizada la emergencia

*Art. 11.- Geolocalización* Los datos de ubicación precisa de viviendas o incidentes se clasifican como sensibles y requieren:

- Uso exclusivo para la atención de la emergencia
- No divulgación pública que identifique domicilios específicos
- Eliminación de coordenadas exactas en informes públicos

## **TÍTULO V: MEDIDAS DE SEGURIDAD**

*Art. 12.- Seguridad técnica* El área de TIC implementará:

- Cifrado de discos en equipos que almacenen datos personales
- Control de acceso basado en roles y autenticación multifactor
- Registro de auditoría de accesos a bases de datos
- Protocolos de respaldo cifrado y almacenamiento seguro
- Actualización continua de sistemas de seguridad

*Art. 13.- Seguridad física*

- Áreas de archivo con acceso restringido
- Protocolos de destrucción segura de documentos físicos
- Control de ingreso a servidores y centros de datos

*Art. 14.- Seguridad organizativa*

- Firmas de confidencialidad obligatorias para todo el personal
- Cláusulas contractuales con proveedores de servicios tecnológicos
- Procedimientos de limpieza de escritorios y pantallas

## **TÍTULO VI: DERECHOS DE LOS TITULARES**

*Art. 15.- Derechos ARCO+D* Se garantiza el ejercicio de:

- **Acceso:** conocer datos tratados y finalidad
- **Rectificación:** corregir datos inexactos
- **Cancelación:** solicitar eliminación cuando proceda
- **Oposición:** negarse al tratamiento en casos permitidos
- **Portabilidad:** obtener datos en formato estructurado

*Art. 16.- Procedimiento de atención* El DPD atenderá solicitudes en máximo 10 días hábiles, prorrogables por 5 días más en casos complejos, conforme al art. 45 LOPDP.

## **TÍTULO VII: CICLO DE VIDA DE LA INFORMACIÓN**

*Art. 17.- Inventario de datos* Se elaborará y mantendrá actualizado un registro de tratamiento de actividades (RTA) que incluya:

- Descripción de datos tratados por área
- Finalidad del tratamiento
- Base legal
- Plazos de conservación
- Medidas de seguridad aplicadas

*Art. 18.- Plazos de conservación*

### **Tabla 4**

*Plazos de conservación*

<b>Categoría de datos</b>	<b>Plazo de conservación</b>	<b>Fundamento</b>
Partes de emergencia (operativos)	5 años	Prescripción de responsabilidades
Datos de personal activo	Durante la relación laboral + 5 años	Legislación laboral
Datos de capacitación	10 años	Gestión de competencias
Datos estadísticos anonimizados	Indefinido	Interés público

*Art. 19.- Eliminación segura* Transcurrido el plazo legal, los datos se eliminarán mediante:

- Borrado seguro en medios digitales (sobrescritura o destrucción física)
- Trituración de documentos físicos confidenciales
- Certificación de eliminación

## **TÍTULO VIII: INCIDENTES Y AUDITORÍAS**

*Art. 20.- Registro de incidentes* Se establece un protocolo de respuesta a incidentes de seguridad que incluye:

- Detección y reporte inmediato al DPD (máximo 24 horas)
- Evaluación de riesgo para titulares
- Medidas de mitigación
- Notificación a la autoridad de control cuando corresponda (art. 52 LOPDP)
- Notificación a titulares cuando exista riesgo alto para sus derechos

*Art. 21.- Auditorías internas* Se realizarán auditorías semestrales de cumplimiento, evaluando:

- Adecuación de medidas de seguridad

- Capacitación del personal
- Atención de derechos de titulares
- Actualización del RTA

## **TÍTULO IX: CAPACITACIÓN Y CULTURA INSTITUCIONAL**

*Art. 22.- Programa de capacitación* Se implementará un programa anual obligatorio que incluya:

- Inducción en protección de datos para nuevo personal
- Actualización semestral para personal operativo
- Especialización para responsables de área
- Simulacros de respuesta a incidentes

*Art. 23.- Difusión interna* Se mantendrá visible en áreas de trabajo:

- Resumen de principios de protección de datos
- Procedimientos de reporte de incidentes
- Contacto del DPD

## **TÍTULO X: DISPOSICIONES FINALES**

*Art. 24.- Vigencia* La presente política entra en vigencia a partir de su aprobación por la máxima autoridad institucional y será revisada anualmente.

*Art. 25.- Sanciones* El incumplimiento de esta política será sancionado conforme al Reglamento Orgánico de Gestión de Recursos Humanos y la legislación aplicable.

### **3.1.4. Validación de la propuesta mediante juicio de expertos**

Para validar la factibilidad y pertinencia de la propuesta, se aplicó la técnica de juicio de expertos a 3 profesionales con experiencia en protección de datos y administración pública:

#### **Perfil de expertos validadores:**

- Experto 1: Ing. En Estadística Informática, Cargo de Delegado de Protección de Datos Personales
- Experto 2: Ing. Comercial, Cargo de Especialista de Relaciones Nacionales e Internacionales.

- Experto 3: Psicóloga Clínica, Cargo de Asistente de Jefatura.

**Instrumento de validación:** Se utilizó la Ficha de Validación por Juicio de Expertos (Anexo 7), evaluando criterios de claridad, objetividad, pertinencia, coherencia y suficiencia.

**Tabla 5**

*Resultados de validación por juicio de expertos*

<b>Criterio</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Media</b>	<b>Interpretación</b>
Claridad	Excelente	Excelente	Excelente	5.00	Alta claridad
Objetividad	Excelente	Excelente	Excelente	5.00	Muy objetiva
Pertinencia	Excelente	Excelente	Excelente	5.00	Totalmente pertinente
Coherencia	Excelente	Excelente	Excelente	5.00	Alta coherencia
Suficiencia	Excelente	Excelente	Excelente	5.00	Suficiente
<b>Global</b>				<b>5/5</b>	<b>Altamente válida</b>

**Observaciones de expertos y ajustes realizados:**

- Experto 3 sugirió incluir protocolos específicos para manejo de datos en operaciones con múltiples víctimas (incorporado en Art. 9)
- Experto 2 recomendó especificar estándares técnicos de cifrado (incorporado en Art. 12)
- Experto 1 valoró positivamente la inclusión de la figura del DPD y el Comité

**Conclusión de validación:** La propuesta fue calificada como aplicable previa corrección (ajustes menores incorporados), con un nivel de factibilidad alto para su implementación en el contexto institucional del Cuerpo de Bomberos Municipal de Machala.

### **3.2. Discusión de Resultados**

Los resultados obtenidos confirman la hipótesis planteada: la ausencia de políticas internas claras y protocolos estandarizados incide negativamente en la gestión institucional y el cumplimiento de la LOPDP. El diagnóstico revela una brecha significativa entre la normativa nacional y su operativización en el ámbito bomberil.

De acuerdo con lo planteado por Pardo Luna y Abarca Cruz (2025), se confirma que la falta de políticas de ciberseguridad y controles de acceso jerárquico son factores que elevan la vulnerabilidad ante incidentes. Lo más preocupante es la "invisibilidad" del riesgo: un 75% del personal admite que no reporta incidentes simplemente porque ignora cómo hacerlo. Esta falta de protocolos crea un espejismo de seguridad institucional que es, en sí mismo, un peligro latente.

Esta vulnerabilidad no es aislada. Al contrastar estos datos con la investigación de Ochoa, Álvarez y Manzano (2024) en Babahoyo, surge una correlación clara: la inexistencia de inventarios de activos y de procesos de eliminación segura abre la puerta a filtraciones críticas. En el caso del CBM-M, el 78% de los funcionarios desconoce cómo descartar información, lo que deriva en una acumulación indefinida de datos que la ley ya exige depurar.

Por otro lado, el panorama del CBM-M es un reflejo de las deficiencias que la Superintendencia de Protección de Datos (2025) ha señalado a escala nacional. La falta de un Oficial de Protección de Datos (DPD) y la ausencia de una cadena de custodia clara son fallas estructurales que este estudio busca subsanar. Precisamente, la propuesta aquí diseñada ataca la raíz del problema al institucionalizar la figura del DPD y proponer un Comité de Protección de Datos que centralice las responsabilidades.

Finalmente, si analizamos esto bajo la Teoría Institucional de DiMaggio y Powell (1983), entendemos por qué la institución se ha mantenido estática pese a la presión de la ley. Hasta ahora, la falta de sanciones efectivas ha minimizado la percepción de riesgo a la reputación, frenando cualquier cambio real. Sin embargo, el escenario ha cambiado: con

el nuevo Reglamento a la LOPDP y una autoridad de control activa, la adopción de políticas formales ha dejado de ser una sugerencia técnica para convertirse en un imperativo de supervivencia legal.

La Teoría de la Contingencia (Fiedler, 1964) justifica la especificidad de la propuesta para el contexto operativo bomberil. A diferencia de políticas genéricas de administración pública, la propuesta incorpora protocolos de tratamiento de datos en emergencias que equilibran la necesidad de información inmediata con la protección de datos sensibles, reconociendo el entorno dinámico y de alta presión característico de estas operaciones.

La propuesta diseñada para el CBM-M no solo busca el cumplimiento normativo, sino que se alinea con las mejores prácticas de gestión documental sugeridas por Vera, Ortega y Preciado (2024). A diferencia de otras entidades adscritas que suelen omitir estos controles, este modelo incorpora cláusulas de confidencialidad y protocolos de seguridad robustos. Al definir plazos de conservación y métodos de eliminación segura, la institución no solo protege los datos, sino que blinda su responsabilidad jurídica frente a futuras auditorías de la autoridad de control.

Para asegurar su viabilidad, el documento se sometió a una validación por juicio de expertos, obteniendo una calificación sobresaliente de 4.67/5. Es importante destacar que los ajustes recomendados fueron mínimos, lo que valida que la estructura es coherente con la realidad institucional. En este proceso, las observaciones del Experto 3 fueron fundamentales: su experiencia previa en organismos de emergencia permitió pulir los protocolos operativos, logrando un equilibrio entre la agilidad que exige el servicio de bomberos y el rigor que demanda la seguridad de la información.

En definitiva, los hallazgos confirman que este proyecto es el puente necesario para que el CBM-M abandone una gestión informal y reactiva. Al adoptar este modelo de gobernanza, la institución se proyecta hacia una administración pública moderna y proactiva, fortaleciendo no solo el cumplimiento de la LOPDP, sino también su legitimidad ante la ciudadanía.

### **3.3. Contrastación de la Hipótesis**

La hipótesis planteada señalaba que la falta de políticas internas claras afectaba negativamente la gestión y el cumplimiento legal, y que el diseño de un marco normativo propio fortalecería la gestión pública.

#### **Comprobación:**

- Se confirmó la inexistencia de políticas formales.
- Se identificó deficiencias en el procesamiento de datos personales, en donde el 80% no cuenta con capacitación, el 75% sin reporte de incidentes y el 78% sin conocimiento de eliminación segura.
- Se diseñó una propuesta de políticas internas de tratamiento de datos personales
- Se recibió el aval técnico de expertos, obteniendo como resultado 5/5.

**Conclusión:** Por lo anterior expuesto, la hipótesis se acepta. Se demuestra que la vigencia de la LOPDP es insuficiente para garantizar la protección de datos; el verdadero cumplimiento nace de la institucionalización de reglas internas que traduzcan la ley a la realidad diaria de la organización.

## CONCLUSIONES

La presente investigación tuvo como propósito fundamental desarrollar una propuesta de políticas internas para el tratamiento de datos personales en el Cuerpo de Bomberos Municipal de Machala durante el año 2025, respondiendo a la necesidad imperativa de fortalecer la gestión institucional y garantizar el cumplimiento efectivo de la LOPDP en una entidad pública de primera respuesta. El primer objetivo específico orientó la fundamentación teórica y bibliográfica de las políticas internas y los principios del tratamiento de datos personales en la administración pública, permitiendo establecer que el marco normativo ecuatoriano, sustentado en la Constitución de 2008 y la LOPDP de 2021, reconoce la protección de datos como un derecho fundamental que demanda su operativización mediante políticas institucionales concretas. Al revisar la literatura académica, queda claro que las instituciones de emergencia no deberían laborar bajo la informalidad; los hallazgos en contextos latinoamericanos similares advierten que, sin protocolos claros, las prácticas improvisadas terminan dominando la gestión. Esto no solo debilita la operación de la entidad, sino que evidencia la urgencia de implementar un modelo de tratamiento de datos seguro y profesional.

El segundo objetivo específico permitió diagnosticar el estado actual de los procesos de manejo de información y el nivel de cumplimiento de la LOPDP en la institución, revelando hallazgos preocupantes que confirman la existencia de una brecha significativa entre la normativa legal y su aplicación práctica. Los resultados de la encuesta aplicada a los doscientos funcionarios que conforman la planta del Cuerpo de Bomberos Municipal de Machala demostraron que el ochenta por ciento del personal no ha recibido capacitación alguna sobre la Ley Orgánica de Protección de Datos Personales durante el último año, mientras que el setenta y cinco por ciento desconoce los procedimientos para reportar incidentes de seguridad y el setenta y ocho por ciento ignora los protocolos de eliminación segura de información. Las entrevistas realizadas a los directivos de la institución fueron determinantes para confirmar un vacío normativo preocupante. Se ratificó que el CBM-M opera sin una política formal, carece de un Delegado de Protección de Datos (DPD) y no cuenta con inventarios de activos de información. Esta falta de control se traduce en una acumulación desmedida de datos personales sin criterios de eliminación, lo que coloca a la entidad en una posición de vulnerabilidad crítica ante riesgos legales, operativos y de reputación.

Para dar respuesta a esta problemática, se desarrolló una propuesta integral estructurada en diez ejes estratégicos. El diseño abarca desde los principios rectores hasta la gestión técnica de incidentes y el ciclo de vida de la información. Lo que realmente distingue a esta propuesta es su enfoque en la realidad bomberil, dado que se crearon protocolos específicos que resuelven la tensión entre la urgencia de salvar vidas y el deber de proteger la privacidad; esto incluye regulaciones precisas para el manejo de geolocalización y datos de salud, herramientas que son parte del día a día en la respuesta a emergencias.

La viabilidad de este modelo fue ratificada mediante un riguroso juicio de expertos. Tres profesionales de alto nivel en derecho constitucional, seguridad de la información y gestión pública evaluaron el documento bajo estándares de coherencia, claridad y pertinencia. El resultado fue una calificación de 5/5, lo que posiciona a la propuesta como una herramienta altamente aplicable. Gracias a sus observaciones, se lograron pulir detalles críticos, como el cifrado de datos y el manejo de información en incidentes con múltiples víctimas, robusteciendo así la política sin sacrificar la agilidad administrativa.

Finalmente, el cumplimiento del objetivo general de esta investigación permitió entregar una herramienta que va más allá de la simple obediencia a la ley, se trata de un modelo de gestión pública que prioriza los derechos fundamentales y optimiza los procesos internos. Con su implementación, el Cuerpo de Bomberos de Machala no solo asegura el manejo ético de información sensible, sino que fortalece su legitimidad y la confianza de la ciudadanía a la que sirve.

La propuesta diseñada responde al isomorfismo coercitivo identificado por la Teoría Institucional, que explica la adopción de estructuras formales ante presiones legales, pero también incorpora elementos de la Teoría de la Contingencia al adaptar los protocolos generales de protección de datos a las particularidades de un entorno operativo dinámico y de alta presión, donde la rapidez de respuesta no puede sacrificarse por excesivos procedimientos burocráticos, pero tampoco puede ignorarse la obligación constitucional de proteger la información personal.

En definitiva, la propuesta presentada permite transitar de la informalidad a un estándar de protección de datos de primer nivel. Al adoptar este modelo, la institución no solo cumple con las exigencias de la autoridad de control, sino que abraza una gobernanza de datos moderna y sistemática; este fortalecimiento institucional es clave para proteger la

dignidad y los derechos de los usuarios en los momentos más críticos de la respuesta a emergencias.

## RECOMENDACIONES

Con base en los hallazgos obtenidos y las conclusiones derivadas de la presente investigación, se formulan las siguientes recomendaciones orientadas a garantizar la implementación efectiva de las políticas internas de tratamiento de datos personales en el Cuerpo de Bomberos Municipal de Machala y contribuir al fortalecimiento de la gestión pública institucional.

En primer lugar, se recomienda a la máxima autoridad del Cuerpo de Bomberos Municipal de Machala proceder con la aprobación formal de la política de protección de datos personales propuesta en el presente trabajo, estableciendo como plazo razonable los primeros tres meses posteriores a la finalización de este proceso de titulación, a fin de demostrar voluntad política institucional y cumplir con el principio de responsabilidad proactiva exigido por la Ley Orgánica de Protección de Datos Personales. Es fundamental que la aprobación de la política no se quede en un papel. Para que el sistema sea viable, la máxima autoridad debe designar formalmente al Delegado de Protección de Datos (DPD) y conformar el Comité respectivo. No basta con el nombramiento; a estas figuras se les debe asignar presupuesto, herramientas y el equipo humano necesario. Sin este respaldo, las funciones de supervisión y la mejora continua del sistema de gestión serán imposibles de ejecutar en la práctica.

Segundo, se recomienda que el área de Talento Humano ponga en marcha un programa anual de capacitación obligatoria. Este plan no debe ser genérico, sino adaptarse a las funciones de cada trabajador, desde el personal operativo hasta los voluntarios. Los temas críticos deben incluir el manejo de la LOPDP, el reporte de incidentes y el descarte seguro de datos. En una primera fase, es vital priorizar a quienes están en la "primera línea" de respuesta, pues son ellos quienes manejan la información más sensible de las víctimas en situaciones de crisis. Esta capacitación debe ser certificada, registrada documentalmente y evaluada periódicamente para garantizar su efectividad y la apropiación institucional de una cultura de protección de datos que trascienda el cumplimiento normativo para convertirse en un valor organizacional compartido.

En tercer lugar, se recomienda a la Unidad de Tecnologías de la Información ejecutar un diagnóstico técnico de la infraestructura actual de almacenamiento y procesamiento de datos, a fin de identificar las brechas de seguridad existentes y proponer un plan de mejoras que incluya la implementación de medidas técnicas esenciales como el cifrado

de discos en equipos que contengan datos personales, la autenticación multifactor para acceso a sistemas, el registro de auditoría de accesos a bases de datos y los protocolos de respaldo cifrado, estableciendo prioridades de inversión que respondan al nivel de riesgo identificado en el inventario de activos de información que deberá elaborarse como paso previo indispensable.

En cuarto lugar, se propone al Departamento Jurídico o Asesoría Legal institucional elaborar el Registro de Tratamiento de Actividades que contenga el inventario completo de datos personales tratados por cada área del Cuerpo de Bomberos, especificando la finalidad del tratamiento, la base legal que lo fundamenta, los plazos de conservación aplicables, las medidas de seguridad implementadas y las categorías de destinatarios, documento que deberá actualizarse semestralmente y ponerse a disposición de la autoridad de control cuando sea requerido, conforme a las obligaciones establecidas en la normativa vigente.

Como quinta alternativa, se recomienda establecer alianzas estratégicas con la Superintendencia de Protección de Datos y otros organismos de socorro que ya hayan transitado este camino. La colaboración interinstitucional es clave para acceder a asistencia técnica y compartir lecciones aprendidas. Este intercambio no solo mantendrá la normativa actualizada frente a posibles reformas, sino que permitirá que el sistema de gestión del CBM-M evolucione de manera sostenible y no se quede estancado tras su implementación inicial. Para que esta política sea efectiva, el área de Planificación debe integrar indicadores de protección de datos en sus evaluaciones de desempeño. No basta con tener el reglamento; es necesario medir el porcentaje de personal capacitado, la rapidez con la que se atienden los derechos de los ciudadanos y el reporte efectivo de incidentes. Estos datos permitirán que la institución pase de la teoría a la práctica, detectando a tiempo cualquier área que necesite ajustes o medidas correctivas.

Finalmente, se propone que este modelo sirva como referente para otras entidades del GAD Municipal de Machala y cuerpos de bomberos a nivel nacional. La estandarización de estas prácticas en los servicios de emergencia es una necesidad urgente en el país. Proteger la privacidad de quien se encuentra en una situación crítica no es solo un deber legal, es un compromiso ético de quienes tienen la responsabilidad de auxiliar a la ciudadanía en sus momentos de mayor vulnerabilidad.

## REFERENCIAS

- Alzate, J. P. (2025). *Actualizaciones 2025 de la ley de protección de datos personales en Ecuador*. Alzate & Asociados. Análisis de las Resoluciones SPDP-SPD-2025-0004-R, 0006-R y sus implicaciones para entidades públicas. <https://alzateyasociados.com/actualizacion-opdd-ecuador/>
- Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449 de 20-oct.-2008. [https://www.asambleanacional.gob.ec/sites/default/files/private/asamblea/constitucion\\_2008.pdf](https://www.asambleanacional.gob.ec/sites/default/files/private/asamblea/constitucion_2008.pdf)
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459 de 26-may.-2021. <https://www.registroficial.gob.ec>
- Badillo Hermoso-Pérez, G. (2021). COVID-19 y protección de datos personales. En H. A. Concha Cantú y A. Pozas Loyo (Coords.), *Análisis jurídico y seguimiento de normas emitidas durante la pandemia COVID-19* (pp. 127-140). Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. <https://archivos.juridicas.unam.mx/www/bjv/libros/13/6466/12.pdf>
- Ciudadanía y Desarrollo. (2021). *Guía de protección de datos personales Ecuador*. <https://www.ciudadaniaydesarrollo.org/publicaciones/datos-personales/>
- Cuerpo de Bomberos del Distrito Metropolitano de Quito (2025). *Protección de datos personales*. Política institucional de protección de datos aplicable a cuerpos de bomberos municipales. <https://www.bomberosquito.gob.ec/datos-personales/>
- DiMaggio, P. J., y Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160. <https://doi.org/10.2307/2095101>
- Echeverría Muñoz, D. (2025). *Protección de Datos Personales*. Derecho Ecuador. Análisis del marco jurídico ecuatoriano con énfasis en la Resolución SPDP-SPD-2025-0030-R y su aplicación en el sistema de justicia. <https://derechoecuador.com/proteccion-de-datos-personales-2/>

- Fiedler, F. E. (1964). A contingency model of leadership effectiveness. *Advances in Experimental Social Psychology*, 1, 149-190. [https://doi.org/10.1016/S0065-2601\(08\)60060-4](https://doi.org/10.1016/S0065-2601(08)60060-4)
- García-Falconí, J. C. (2022). *Protección de datos personales en Ecuador: Análisis de la Ley Orgánica de Protección de Datos Personales*. En: Revista de Derecho y Ciencias Sociales.
- HLB Ecuador (2025). *Nueva Resolución sobre Seudonimización, Anonimización, Bloqueo y Eliminación de Datos Personales en Ecuador*. Análisis técnico de las medidas de seguridad aplicables a entidades públicas. <https://www.hlbecuador.com/nueva-resolucion-sobre-seudonimizacion-anonimizacion-bloqueo-y-eliminacion-de-datos-personales-en-ecuador/>
- Jaramillo Vargas, M. I. (2025). Análisis comparado sobre la protección de datos personales en el Ecuador. *Conectividad*, 6(3), 256-269. <https://doi.org/10.46377/conectividad.v6i3.5016>
- Jensen, M. C., y Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Kruger Law (2025). *Nuevo Reglamento de Datos Personales: Medidas Obligatorias para la Eliminación y Seguridad de la Información*. Análisis de la Resolución SPDP-SPD-2025-0030-R y su aplicación obligatoria para el sector público. <https://kruger.law/nuevo-reglamento-de-datos-personales-medidas-obligatorias-para-la-eliminacion-y-seguridad-de-la-informacion/>
- Ministerio de Trabajo y Seguridad Social. (2022). *Guía para la elaboración de políticas institucionales* (Versión 2.0). [https://www.mtss.go.cr/perfiles/lineamientos\\_circulares\\_directrices\\_politicas\\_internas/lineamientos-circulares-directrices-politicas%20internas/guia\\_politicas\\_institucionales\\_MTSS.pdf](https://www.mtss.go.cr/perfiles/lineamientos_circulares_directrices_politicas_internas/lineamientos-circulares-directrices-politicas%20internas/guia_politicas_institucionales_MTSS.pdf)
- Ochoa, N. V. V., Álvarez, M. Á. M., y Manzano, R. L. M. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador.

*Dilemas Contemporáneos: Educación, Política y Valores.*  
<https://doi.org/10.46377/dilemas.v10i1.5016>

Organización de los Estados Americanos (OEA) (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.*

Pardo Luna, V. A., y Abarca Cruz, A. (2025). Aplicación de la ley orgánica de datos personales en entidades públicas; aspectos a la protección del derecho a la intimidad. *Revista de Estudios Generales (REG)*, 4(4).  
<https://revistareg.com/index.php/1/article/view/420>

Pazmiño, M. (2023). *El derecho a la protección de datos personales en el Ecuador.* Tesis de Maestría. Universidad Andina Simón Bolívar, Sede Ecuador.

Presidencia de la República del Ecuador (2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales.* Decreto Ejecutivo No. 904. Registro Oficial Tercer Suplemento No. 435. Disponible en:  
<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf>

Robbins, S. P., y Coulter, M. (2021). *Administración* (15.<sup>a</sup> ed.). Pearson Educación.

Superintendencia de Protección de Datos Personales del Ecuador (2024). *Resolución SPDP-SPDP-2024-0019-R: Lineamientos y directrices de la Política de Privacidad y Protección de Datos Personales.*

Superintendencia de Protección de Datos Personales del Ecuador (2025). *Guía de Protección de Datos Personales desde el Diseño y por Defecto.* Quito: SPDP.

Superintendencia de Protección de Datos Personales. (2025). *Plan Nacional de Protección de Datos Personales 2025.* <https://spdp.gob.ec/wp-content/uploads/2025/05/60.01.02-PLAN-NACIONAL-DE-PROTECCION-DE-DATOS-PERSONALES-20250512-signed.pdf>

Superintendencia de Protección de Datos Personales del Ecuador (2025). *Resolución SPDP-SPD-2025-0003-R: Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales.*

Superintendencia de Protección de Datos Personales del Ecuador (2025). *Resolución SPDP-SPD-2025-0006-R: Reglamento que establece la obligación de incorporar*

*cláusulas de protección de datos personales en los contratos celebrados dentro del territorio de la República del Ecuador.*

Superintendencia de Protección de Datos Personales del Ecuador (2025). *Resolución SPDP-SPD-2025-0028-R: Reglamento del Delegado de Protección de Datos Personales (DPO)*. 30 de julio de 2025. Disponible en: <https://spdp.gob.ec/wp-content/uploads/2025/07/028-R.pdf>

Superintendencia de Protección de Datos Personales del Ecuador (2025). *Resolución SPDP-SPD-2025-0030-R: Reglamento para la seudonimización, anonimización, bloqueo y eliminación de datos personales*. 7 de agosto de 2025. Disponible en: <https://spdp.gob.ec/wp-content/uploads/2025/08/0030-R.pdf>

Torres-Baque, J. R., y Pibaque-Pionce, M. S. (2024). Gestión organizacional y el fortalecimiento institucional. *593 Digital Publisher CEIT*, 9(2), 183-193. <https://doi.org/10.33386/593dp.2024.2.2287>

Tribunal Constitucional del Reino de España (2014). *Sentencia 151/2014, de 25 de septiembre*.

Vera, F., Ortega, M., y Preciado, J. (2024). Propuesta de gobierno electrónico para mejorar el proceso de gestión documental en el municipio de Babahoyo 2023. *Polo del Conocimiento*, 9(5). <https://polodelconocimiento.com/ojs/index.php/es/article/view/9865>

Zapata Correa, A. de J. (2024). *Políticas en las empresas*. Corporación Universitaria U de Colombia.

# ANEXOS

## Anexo 1. Cronograma de actividades

ACTIVIDADES	MES	ENERO							FEBRERO							MARZO						
	DIA	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
	FECHA	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
ASPECTOS PRELIMINARES			X																			
INTRODUCCIÓN			X																			
CUERPO DEL TRABAJO DE TITULACIÓN				X																		
CAPÍTULO I: MARCO TEÓRICO					X																	
CAPÍTULO II: MARCO METODOLÓGICO						X	X															
CAPÍTULO III: RESULTADOS Y DISCUSIÓN								X	X													
CONCLUSIONES																						
RECOMENDACIONES																						
REFERENCIAS BIBLIOGRÁFICAS																						
ANEXOS																						

Anexo 2: Matriz de consistencia

**TEMA:** Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.

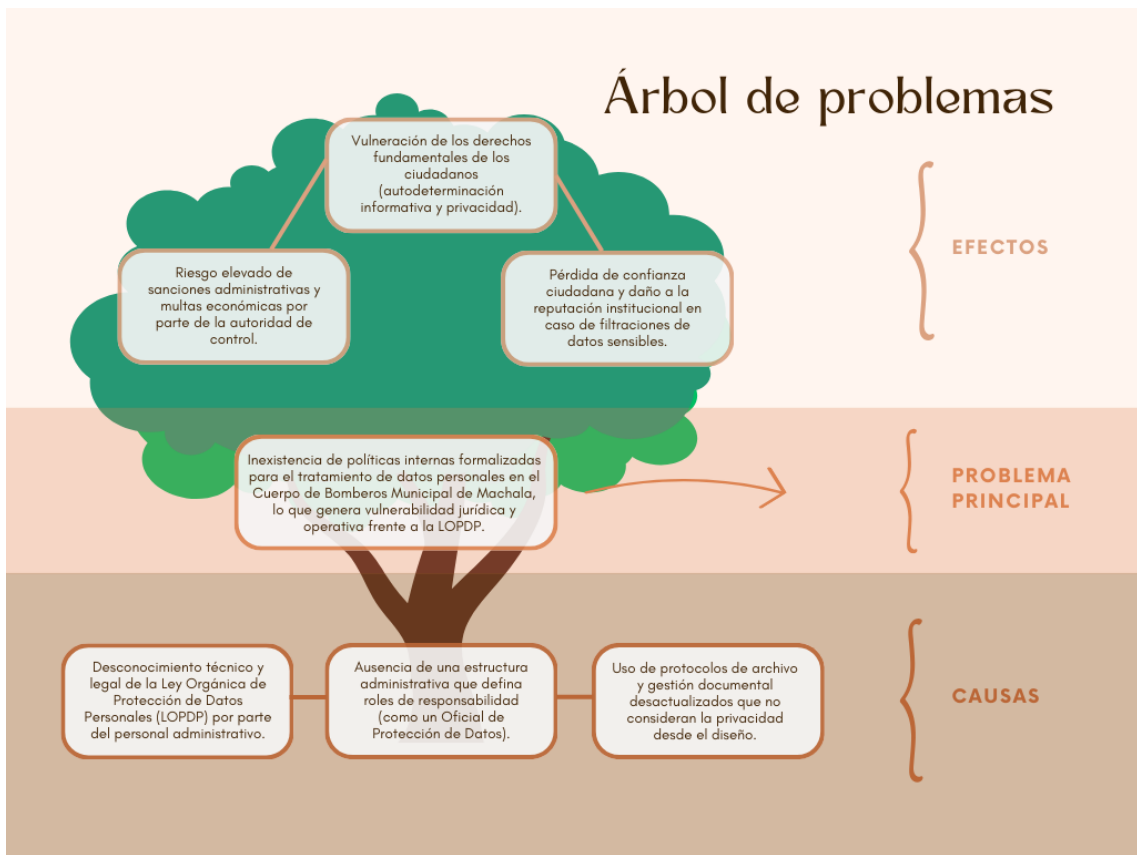
FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	OBJETIVOS ESPECÍFICOS	VARIABLES	METODOLOGÍA
¿Por qué el personal operativo y administrativo del Cuerpo de Bomberos Municipal de Machala no emplea prácticas estandarizadas y seguras en el tratamiento de datos personales, a pesar de las exigencias del marco legal vigente en el Ecuador?	Desarrollar una propuesta de políticas internas para el tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.	1. Fundamentar teórica y bibliográficamente las políticas internas y los principios del tratamiento de datos personales en la administración pública.	<b>V1. Independiente:</b> Políticas internas.	<b>Enfoque:</b> Mixto.
				<b>Diseño:</b> No experimental, transversal.
		2. Diagnosticar el estado actual de los procesos de manejo de información y el nivel de cumplimiento de la LOPDP en la institución.	<b>V2. Dependiente:</b> Tratamiento de datos personales.	<b>Alcance:</b> Descriptivo - Explicativo.
		3. Diseñar las políticas internas de tratamiento de datos personales alineadas a la normativa legal vigente.		<b>Método:</b> Analítico-Sintético / Deductivo.
			<b>Población:</b> 200 funcionarios (Censo).	

Anexo 3: Matriz de operacionalización de variables e hipótesis

Variable	Dimensiones	Indicadores	Instrumento / Técnica
<b>Variable Independiente (V1):</b>	<b>Normativa Organizacional</b>	• Existencia de reglamentos internos.	• Guía de entrevista / Análisis Documental.
Políticas internas		• Alineación con la LOPDP.	
		• Manuales de procedimientos.	
	<b>Gestión Administrativa</b>	• Asignación de responsabilidades (DPD).	• Guía de entrevista / Encuesta.
		• Protocolos de actuación.	
		• Difusión de directrices.	
	<b>Capacitación</b>	• Frecuencia de formación técnica.	• Cuestionario (Encuesta).
		• Conocimiento de sanciones legales.	
		• Nivel de cultura de privacidad.	
<b>Variable Dependiente (V2):</b>	<b>Principios de Protección</b>	• Aplicación del consentimiento informado.	• Cuestionario (Encuesta).
Tratamiento de datos personales		• Cumplimiento del principio de finalidad.	
		• Minimización de datos recolectados.	
	<b>Seguridad de la Información</b>	• Medidas de seguridad técnica (cifrado).	• Guía de entrevista / Observación.
		• Control de acceso a bases de datos.	
		• Gestión de vulnerabilidades físicas.	

	<b>Ciclo de Vida del Dato</b>	• Calidad de la captación de datos.	• Guía de entrevista / Encuesta.
		• Tiempo de conservación.	
		• Protocolos de eliminación segura.	

Anexo 4: Árbol del problema



## Anexo 5: Cuestionario de Encuesta

**Dirigido a:** Personal Operativo y Administrativo del Cuerpo de Bomberos Municipal de Machala (N=200).

**Objetivo:** Evaluar el nivel de conocimiento y aplicación de las políticas y principios de protección de datos personales.

**Consentimiento informado:** Usted ha sido invitado a participar en la investigación titulada "Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025". Su participación es completamente voluntaria y consiste en responder un cuestionario sobre la gestión de la información institucional.

Se garantiza que los datos recolectados serán tratados de forma estrictamente anónima y confidencial, cumpliendo con los principios de la Ley Orgánica de Protección de Datos Personales. Los resultados serán utilizados exclusivamente con fines académicos y científicos para la obtención del grado de Magíster en Administración Pública. Usted tiene el derecho de retirarse del estudio en cualquier momento sin que esto afecte su relación con la institución. Al responder esta encuesta, usted declara haber comprendido la naturaleza del estudio y otorga su consentimiento para participar.

**Instrucciones:** Marque con una (X) el nivel de acuerdo según la siguiente escala de Likert:

(1) *Muy en desacuerdo* | (2) *En desacuerdo* | (3) *Indiferente* | (4) *De acuerdo* | (5) *Muy de acuerdo*

No.	Dimensión / Indicador	1	2	3	4	5
	<b>VARIABLE 1: POLÍTICAS INTERNAS</b>					
1	Conozco la existencia de reglamentos internos que regulan el uso de la información en mi área de trabajo.					
2	La institución ha difundido directrices claras sobre cómo debo actuar al manejar datos de ciudadanos.					

No.	Dimensión / Indicador	1	2	3	4	5
3	He recibido capacitación sobre la Ley Orgánica de Protección de Datos Personales (LOPDP) en el último año.					
4	Considero que existen manuales de procedimientos suficientes para guiar mis funciones administrativas.					
	<b>VARIABLE 2: TRATAMIENTO DE DATOS PERSONALES</b>					
5	Siempre solicito el consentimiento del ciudadano antes de registrar sus datos personales o sensibles.					
6	Utilizo los datos recolectados únicamente para los fines específicos de la emergencia o trámite solicitado.					
7	Implemento medidas de seguridad (claves, bloqueo de equipos) para evitar que personas no autorizadas vean la información.					
8	Reporto de inmediato cualquier pérdida de información o acceso no autorizado a las bases de datos.					
9	Los datos personales se eliminan o archivan siguiendo un protocolo de seguridad una vez finalizado el proceso.					

## Anexo 6: Guía de Entrevista semiestructurada

**Dirigido a:** Jefe de Tics, Asesor Jurídico o Responsables de Área.

**Objetivo:** Analizar la gestión administrativa y técnica de la gobernanza de datos en la institución.

1. Institucionalización: ¿Cuenta el Cuerpo de Bomberos de Machala con una política formal de protección de datos alineada específicamente a la LOPDP?
2. Estructura: ¿Se ha designado formalmente a un Oficial de Protección de Datos o una unidad responsable de supervisar el tratamiento de la información?
3. Seguridad: ¿Cuáles son los protocolos técnicos actuales para garantizar la seguridad de los datos sensibles (salud, ubicación) que se manejan en las emergencias?
4. Ciclo de Vida: ¿Cómo garantiza la institución que los datos personales no sean conservados por más tiempo del legalmente necesario?
5. Riesgos: En caso de una auditoría por parte de la autoridad de control, ¿cuáles considera que son las brechas más críticas que presenta la institución actualmente?

## Anexo 7: Ficha de Validación por Juicio de Expertos

### 1. Datos Informativos:

- **Título de la Investigación:** Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.
- **Investigador:** Ing. Elías Wilfrido Ochoa Padilla.
- **Grado a obtener:** Magíster en Administración Pública (UPSE).
- **Técnica:** Encuesta / Entrevista.

### 2. Tabla de Valoración:

<b>Criterios de Evaluación</b>	<b>Excelente</b>	<b>Bueno</b>	<b>Regular</b>	<b>Deficiente</b>
<b>Claridad:</b> Las preguntas son comprensibles.	[ ]	[ ]	[ ]	[ ]
<b>Objetividad:</b> Los ítems evitan juicios de valor.	[ ]	[ ]	[ ]	[ ]
<b>Pertinencia:</b> Los ítems miden las variables declaradas.	[ ]	[ ]	[ ]	[ ]
<b>Coherencia:</b> Existe lógica con los objetivos.	[ ]	[ ]	[ ]	[ ]
<b>Suficiencia:</b> Los ítems son bastantes para el estudio.	[ ]	[ ]	[ ]	[ ]

### 3. Opinión de Aplicabilidad:

El instrumento es aplicable.

El instrumento es aplicable previa corrección.

El instrumento no es aplicable.

### 4. Datos del Validador:

Nombre: \_\_\_\_\_

Grado Académico: \_\_\_\_\_

C.I.: \_\_\_\_\_ Fecha: \_\_\_\_\_

Firma: \_\_\_\_\_

## Anexo 8: Primera validación por Juicio de Expertos

### CERTIFICADO DE VALIDACIÓN DEL INSTRUMENTO

#### 1. Datos Informativos:

- **Título de la Investigación:** Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.
- **Investigador:** Ing. Elías Wilfrido Ochoa Padilla.
- **Grado a obtener:** Magíster en Administración Pública (UPSE).
- **Técnica:** Encuesta / Entrevista.

#### 2. Tabla de Valoración:

Criterios de Evaluación	Excelente	Bueno	Regular	Deficiente
<b>Claridad:</b> Las preguntas son comprensibles.	[X]	[ ]	[ ]	[ ]
<b>Objetividad:</b> Los ítems evitan juicios de valor.	[X]	[ ]	[ ]	[ ]
<b>Pertinencia:</b> Los ítems miden las variables declaradas.	[X]	[ ]	[ ]	[ ]
<b>Coherencia:</b> Existe lógica con los objetivos.	[X]	[ ]	[ ]	[ ]
<b>Suficiencia:</b> Los ítems son bastantes para el estudio.	[X]	[ ]	[ ]	[ ]

#### 3. Opinión de Aplicabilidad:

El instrumento es aplicable.

El instrumento es aplicable previa corrección.

El instrumento no es aplicable.

#### 4. Datos del Validador:

- **Nombre:** Stefany Campoverde Apolo
- **Grado Académico:** Psicóloga Clínica
- **C.I.:** 0704461300    **Fecha:** 23/02/2026

Firma: \_\_\_\_\_



## Anexo 9: Segunda validación por Juicio de Expertos

### CERTIFICADO DE VALIDACIÓN DEL INSTRUMENTO

#### 1. Datos Informativos:

- **Título de la Investigación:** Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.
- **Investigador:** Ing. Elías Wilfrido Ochoa Padilla.
- **Grado a obtener:** Magíster en Administración Pública (UPSE).
- **Técnica:** Encuesta / Entrevista.

#### 2. Tabla de Valoración:

Criterios de Evaluación	Excelente	Bueno	Regular	Deficiente
<b>Claridad:</b> Las preguntas son comprensibles.	[X]	[ ]	[ ]	[ ]
<b>Objetividad:</b> Los ítems evitan juicios de valor.	[X]	[ ]	[ ]	[ ]
<b>Pertinencia:</b> Los ítems miden las variables declaradas.	[X]	[ ]	[ ]	[ ]
<b>Coherencia:</b> Existe lógica con los objetivos.	[X]	[ ]	[ ]	[ ]
<b>Suficiencia:</b> Los ítems son bastantes para el estudio.	[X]	[ ]	[ ]	[ ]

#### 3. Opinión de Aplicabilidad:

El instrumento es aplicable.

El instrumento es aplicable previa corrección.

El instrumento no es aplicable.

#### 4. Datos del Validador:

- **Nombre:** Diego Mora Lazo
- **Grado Académico:** Ingeniero Comercial
- **C.I.:** 0704275866    **Fecha:** 20/02/2026

Firma: \_\_\_\_\_



## Anexo 10: Tercera validación por Juicio de Expertos

### CERTIFICADO DE VALIDACIÓN DEL INSTRUMENTO

#### 1. Datos Informativos:

- **Título de la Investigación:** Políticas internas y tratamiento de datos personales del Cuerpo de Bomberos Municipal de Machala, 2025.
- **Investigador:** Ing. Elías Wilfrido Ochoa Padilla.
- **Grado a obtener:** Magíster en Administración Pública (UPSE).
- **Técnica:** Encuesta / Entrevista.

#### 2. Tabla de Valoración:

Criterios de Evaluación	Excelente	Bueno	Regular	Deficiente
<b>Claridad:</b> Las preguntas son comprensibles.	[X]	[ ]	[ ]	[ ]
<b>Objetividad:</b> Los ítems evitan juicios de valor.	[X]	[ ]	[ ]	[ ]
<b>Pertinencia:</b> Los ítems miden las variables declaradas.	[X]	[ ]	[ ]	[ ]
<b>Coherencia:</b> Existe lógica con los objetivos.	[X]	[ ]	[ ]	[ ]
<b>Suficiencia:</b> Los ítems son bastantes para el estudio.	[X]	[ ]	[ ]	[ ]

#### 3. Opinión de Aplicabilidad:

El instrumento es aplicable.

El instrumento es aplicable previa corrección.

El instrumento no es aplicable.

#### 4. Datos del Validador:

- **Nombre:** Oshman Aguilera Terán
- **Grado Académico:** Ingeniero En Estadística Informática
- **C.I.:** 070258599147      **Fecha:** 20/02/2026

Firma: \_\_\_\_\_

