Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XI Número: 2 Artículo no.:66 Período: 1 de enero al 30 de abril del 2024

TÍTULO: 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.

AUTORES:

1. Máster. Nelly Valeria Vinueza Ochoa.
2. Est. Miguel Ángel Macías Álvarez.
3. Máster. Rosa Leonor Maldonado Manzano.

RESUMEN: En Ecuador, es imperativo priorizar la gestión de datos personales y mejorar de inmediato la seguridad de los usuarios frente a las crecientes amenazas de filtración de datos y la falta de eficacia en la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPD). Este estudio tuvo como objetivo analizar, evaluar y proponer estrategias integrales de seguridad de la información y principios de conservación efectivos para el manejo de datos personales en las instituciones públicas de la ciudad de Babahoyo. Como conclusión, se destaca la necesidad de implementar de manera sistemática medidas ejecutivas que permitan una gestión y tratamiento adecuados de los datos personales de los ciudadanos por parte de la administración pública.

PALABRAS CLAVES: seguridad, información, gestión de datos personales, usuarios, filtración de datos.

TITLE: Implementation of security measures and principle of data retention according to the organic law of personal data protection in public institutions of Babahoyo, Ecuador.

AUTHORS:

1. Master. Nelly Valeria Vinueza Ochoa
2. Stud. Miguel Ángel Macías Álvarez
3. Master. Rosa Leonor Maldonado Manzano.

ABSTRACT: In Ecuador, it is imperative to prioritize the management of personal data and immediately improve the security of users in the face of growing threats of data leakage and the lack of effectiveness in the application of the Organic Law for the Protection of Personal Data (LOPD). The objective of this study was to analyze, evaluate and propose comprehensive information security strategies and effective conservation principles for the management of personal data in public institutions in the city of Babahoyo. As a conclusion, it highlights the need to systematically implement executive measures that allow an adequate management and treatment of citizens' personal data by the public administration.

KEY WORDS: security, information, personal data management, users, data leakage.

INTRODUCCIÓN.

La Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP) establece medidas de seguridad y el principio de conservación de datos para garantizar la protección de los datos personales (Rovira et al., 2023). Según la ley, las empresas deben implementar medidas y controles de seguridad que sean el resultado de un análisis de riesgos y una evaluación de impacto; además, se debe mantener actualizado el Registro Nacional de Protección de Datos Personales, al informar la identificación de la base de datos, la naturaleza de los datos tratados, el tiempo de conservación de los datos, y la existencia de transferencias internacionales (Durán & Zamora, 2023).

La Ley Orgánica de Protección de Datos Personales (LOPD) estableció un "Período de adaptación de dos años", que concluyó el 26 de mayo del 2023; sin embargo, su impacto inmediato en el país fue

limitado, lo que generó vulneraciones a los derechos de los titulares de la información al carecer de una tutela efectiva por parte de las instituciones responsables (Cevallos & Delgado, 2023).

La urgencia en Ecuador de priorizar el tratamiento de datos personales y fortalecer la seguridad del usuario es evidente, al considerar las crecientes amenazas de filtración y la falta de eficacia en la aplicación de la LOPD. Este incumplimiento legal expone a los propietarios de la información a diversos riesgos, como suplantación de identidad, estafas en línea, extorsión, acoso y ciberacoso.

Las instituciones encargadas de la conservación de datos no cumplen plenamente con los principios establecidos en la LOPD, específicamente en lo referente a la supresión o revisión periódica autorizada por el usuario. La seguridad de los datos es un derecho que implica un manejo adecuado desde su autorización, y su conservación debe alinearse con la finalidad original del tratamiento, al evitar intervenciones indebidas en los plazos establecidos.

En el contexto constitucional de Ecuador, la protección de datos personales se erige como un mecanismo jurídico para garantizar el derecho a la vida privada en la era digital (Pesantez-Maura & Torres-Ortuño, 2023). La Constitución ecuatoriana considerada moderna en América Latina, refleja un compromiso con la era digital y las nuevas tecnologías, al establecer la privacidad de los datos personales como un elemento fundamental (Cornejo & Sánchez, 2023); además, la protección de datos en la sociedad de la información de los años 70, destaca la necesidad de adoptar políticas públicas ante el crecimiento del uso de tecnologías de la información.

El tratamiento y protección de datos personales tienen como objetivo principal regular principios, derechos y obligaciones para garantizar a los titulares su derecho a la protección y autodeterminación informativa. El derecho a la protección de datos personales es de reciente consagración y proclama la no injerencia de terceros en la vida privada del individuo.

La Ley Orgánica de Protección de Datos Personales (LOPD) define el tratamiento de datos como cualquier acción sobre información personal, ya sea automatizada, parcial o manual; por ende, la

conservación de datos implica mantener y almacenar información de manera segura, al establecer plazos y políticas para proteger la privacidad del titular.

El derecho a la intimidad de datos personales se basa en la confidencialidad sobre aspectos privados, y la vulneración se traduce en la divulgación no autorizada de información sensible (Rivera & Maldonado, 2023).

La sistematización de este análisis revela, que el proceso de conservación es fundamental para garantizar la preservación y correcta utilización de los datos personales por parte de entidades públicas.

El manejo de la conservación de datos en instituciones es esencial para cumplir con la legislación de protección de datos en Ecuador. A continuación, se analizan cómo las instituciones gestionan la conservación de datos, al considerar plazos y políticas establecidas (ver figura 1).

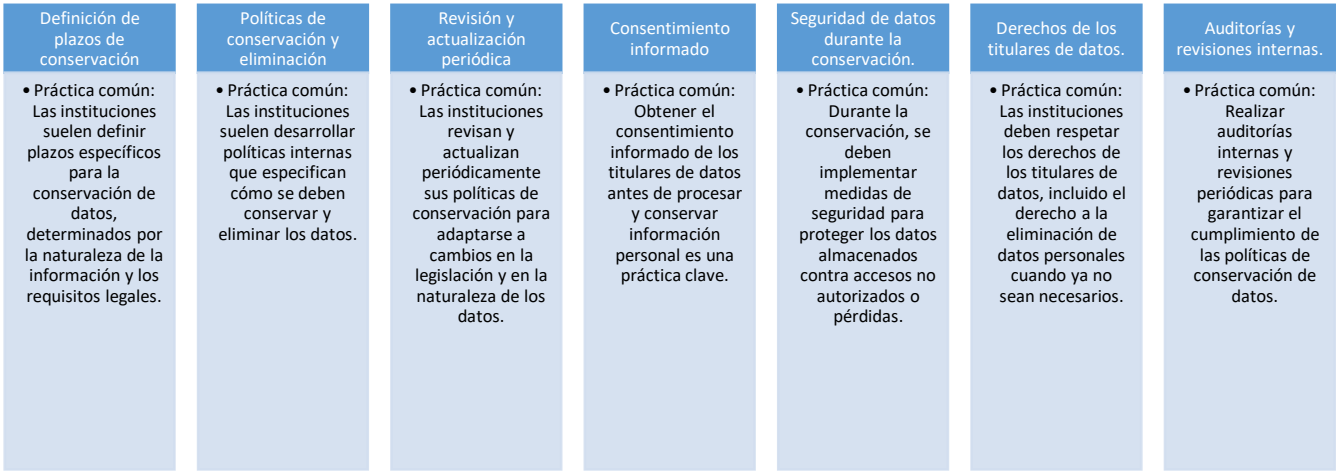

Figura 1. Gestión de la conservación de datos personales por las instituciones.

Fuente**.** Elaboración propia.

En síntesis, el manejo efectivo de la conservación de datos en instituciones implica establecer plazos claros, políticas detalladas, asegurar el consentimiento informado, implementar medidas de seguridad, y respetar los derechos de los titulares de datos. La revisión y actualización periódica de estas prácticas son fundamentales para adaptarse a los cambios en la legislación y la naturaleza de los datos manejados.

El objetivo general del estudio consiste en analizar, evaluar y proponer estrategias integrales de seguridad de la información y principios de conservación efectivos para el manejo de datos personales en las instituciones públicas de la ciudad de Babahoyo, Ecuador. Según lo establece los lineamientos establecidos y en concordancia con la Ley Orgánica de Protección de Datos Personales; para ello, se definen los siguientes objetivos específicos:

- Determinar los desafíos que enfrentan las instituciones públicas en términos de seguridad y conservación de datos.
- Proponer medidas de seguridad para la protección de datos personales.
- Analizar y proponer los conjuntos de estrategias integrales.
- Proponer proyectos claves para el fortalecimiento, seguridad y conservación de datos en instituciones públicas de Babahoyo a partir del análisis del método MOORA.

DESARROLLO.

Materiales y métodos.

Determinación de la población y la muestra.

En el marco de la investigación centrada en la seguridad y el principio de conservación en el procesamiento de información, tal como lo prescribe la Ley Orgánica de Protección de Datos Personales del Ecuador, se enfoca en las instituciones públicas situadas en la ciudad de Babahoyo. Para contextualizar la muestra de esta población, es importante tener en cuenta que Babahoyo posee una población de aproximadamente 170 mil habitantes.

Muestra

$$z = \frac{Z^2 x p x (1 - p)}{E^2}$$

Nivel de confianza (Z): 1,96.

Margen de error (E): 0,05

Estimación de proporción poblacional (p): 0,5.

$$n = \frac{1.96^2 x 0.5 x (1 - 0.5)}{0.05^2}$$

$$n = \frac{3.8416 x 0.25}{0.0025}$$

$$n = \frac{0.9604}{0.0025}$$

$$n = 384.16$$

$$n = 385$$

El tamaño de la muestra es de 385.

Encuesta.

La encuesta fue una forma efectiva de obtener datos directos de las personas involucradas, lo que puede proporcionar una visión más completa y realista de la situación en las instituciones públicas de Babahoyo en relación con la seguridad y la conservación de datos personales.

Entrevista.

Se empleó la entrevista como un instrumento fundamental para recopilar datos cualitativos a operadores jurídicos que manejan los derechos digitales y protección de datos personales para obtener perspectivas directas de los profesionales involucrados en las instituciones públicas de la ciudad de Babahoyo (Grau, 2019).

Método MOORA.

El método Optimización Multiobjetivo por análisis de radio proporción (MOORA, por sus siglas en inglés) fue introducido por Brauers y Zavadskas. La idea básica de este procedimiento es calcular el rendimiento global de cada alternativa o estrategia como la diferencia entre las sumas de sus rendimientos normalizados que pertenecen a los criterios de costo y beneficio (Patnaik et al., 2020).

Antes de iniciar, es importante tener bien definidos todos los atributos y considerar que todos estos deben ser mensurables; es decir, que puedan ser medidos o valorados con respecto a cada una de las alternativas o estrategias (Hasan Hakan & İsmail, 2022). A continuación, se describe detalladamente el procedimiento para la implementación de dicho método.

1. Planteamiento de MDF.

El método comienza con la identificación de alternativas y criterios disponibles. Luego, se construye la matriz de toma de decisiones, que contiene n filas que representan las alternativas o estrategias $A_1, \dots, A_n$ en la evaluación, y J+L las columnas que representan los criterios bajo evaluación (J criterios cuantitativos y L criterios cualitativos). De esta forma, la matriz de decisión final (MDF) se calcula usando la ecuación (1).

$$\text{MDF}=[VO, VST]= \begin{bmatrix} A^1 \\ A^2 \\ \vdots \\ A^n \end{bmatrix} \begin{bmatrix} x_1^1 & \cdots & x_J^1 & x_{J+1}^1 & \cdots & x_{J+L}^1 \\ x_1^2 & \cdots & x_J^2 & x_{J+1}^2 & \cdots & x_{J+L}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^n & \cdots & x_J^n & x_{J+1}^2 & \cdots & x_{J+L}^n \end{bmatrix} \qquad (1)$$

Dónde A_i representan las alternativas o estrategias, para $i = 1 \dots n$, y x_j^i representa las entradas de la alternativa i con respecto al criterio j.

2. Calcular la matriz de decisión normalizada.

Es factible que los criterios de calificación se expresen en diversas unidades o escalas de medida; por lo que la normalización se lleva a cabo, donde la norma euclidiana se obtiene de acuerdo con la ecuación (2) al criterio x_j.

$$|X_j| = \sqrt{\sum_1^n x_i^2} \qquad (2)$$

por lo tanto, la normalización de cada entrada en el MDF se lleva a cabo de acuerdo con la ecuación (3).

$$x_{ij} = \frac{x_{ij}}{|X_j|} \quad (3)$$

Los resultados obtenidos usando ecuación (3) son valores adimensionales que carecen de escala, lo que permite que las operaciones entre los criterios sean aditivas.

3. Calcular la matriz de decisión normalizada ponderada.

Teniendo en cuenta la diferente importancia de los criterios, las calificaciones ponderadas normalizadas Wx_{ij} se calculan con la ecuación (4).

$$Wx_{ij} = w_i \cdot x_{ij} \quad (4)$$

4. Selección de alternativas mediante la distancia a punto de referencia al usar Tchebycheff.

Se construye el punto o alternativa de referencia $R[r_j]$. Este punto de referencia se construye con la mejor evaluación para cada criterio.

Para medir la distancia entre cada alternativa y el punto de referencia se utiliza la métrica de Tchebycheff, según la ecuación (5) y (6).

$$Dist_{(i;j)} = \{max_j|r_j - Wx_{ij}|\} \quad (5)$$

Se ordenan las alternativas de acuerdo con la menor distancia

$$min_i = \{max_j|r_j - Wx_{ij}|\} \quad (6)$$

Resultados.

De los resultados obtenidos en encuestas y entrevistas, se analiza desde la perspectiva legal, ¿cuáles son los 5 desafíos que enfrentan las instituciones públicas en términos de seguridad y conservación de datos en el contexto de la legislación ecuatoriana? A partir de las respuestas obtenidas, se jerarquizó en una escala del 1 al 10 (ver tabla 1), la valoración de los desafíos y qué valor de incidencia posee en el tratamiento de los datos.

Tabla 1. Desafíos que enfrentan las instituciones públicas en términos de seguridad y conservación de datos.

N	Desafíos	Validación en el principio de conservación. (VI)	Repercusión en el tratamiento de los datos. (VD)
1	Cumplimiento de la norma.	8	9
2	Adecuación y oportunidad de medidas de seguridad.	9	9
3	Notificación de incidentes para la toma de decisiones.	7	9
4	Gestión efectiva de los datos	10	10
5	Auditorías internas para precisar los niveles de conservación y tratamiento de los datos.	9	10

Fuente: Elaboración propia.

Desde una perspectiva legal, las instituciones públicas en Ecuador enfrentan cinco desafíos clave en términos de seguridad y conservación de datos, los cuales han sido jerarquizados y valorados del 1 al 10 en función de su importancia en el tratamiento de datos:

1. Cumplimiento de la Ley Orgánica de Protección de Datos Personales: Valoración de 8, con una alta incidencia de 9 en el tratamiento de datos.
2. Adecuación de medidas de seguridad: Valoración de 9, con una relevante incidencia de 9 en el tratamiento de datos.
3. Notificación de incidentes de seguridad: Valoración de 7, con una significativa incidencia de 9 en el tratamiento de datos.
4. Gestión efectiva de los datos: Valoración de 10, con una máxima incidencia de 10 en el tratamiento de datos.

5. Auditorías internas y externas: Valoración de 9, con una máxima incidencia de 10 en el tratamiento de datos.

En cuanto a medidas legales y reglamentarias para fortalecer la protección de datos personales en instituciones públicas, se podrían considerar:

1. Establecer políticas claras de privacidad: Definir reglas y procedimientos para el manejo adecuado de datos personales.
2. Capacitación del personal: Garantizar que el personal esté debidamente formado en prácticas de seguridad de datos.
3. Implementar tecnologías de seguridad avanzadas: Utilizar herramientas modernas para proteger la integridad de la información.
4. Auditorías regulares: Realizar auditorías internas y externas para evaluar la efectividad de las medidas de seguridad implementadas (Minaya et al, 2023).
5. Fomentar la transparencia: Promover la divulgación de las políticas de seguridad y privacidad para generar confianza en los ciudadanos.

La propuesta de un reglamento puede fortalecer la aplicación de la norma jurídica sustantiva y optimizar la seguridad y conservación de datos personales al proporcionar directrices más detalladas y adaptadas a los avances tecnológicos en constante cambio. Esto permitiría una mayor claridad en las prácticas requeridas y facilitaría la adaptación a los desafíos emergentes.

En cuanto a las implicaciones legales de los incidentes de seguridad de datos en instituciones públicas, es esencial abordarlos desde una perspectiva legal. Esto incluiría:

1. Notificación oportuna: Establecer procedimientos claros para informar rápidamente sobre incidentes de seguridad.
2. Investigación interna: Realizar investigaciones internas para determinar la causa y la magnitud del incidente.

3. Coordinación con autoridades: Colaborar con las autoridades pertinentes para abordar las consecuencias legales.
4. Remediación y prevención: Implementar medidas correctivas y preventivas para evitar futuros incidentes.
5. Cumplimiento normativo: Asegurar el cumplimiento de las leyes y regulaciones relacionadas con la seguridad de datos.

Estas acciones contribuirían a mitigar los impactos legales y proteger los derechos de los titulares de datos en el contexto de incidentes de seguridad.

Cumplimiento normativo.

En cuanto al cumplimiento normativo en términos de protección de datos es un desafío constante para muchas instituciones, tanto públicas como privadas a nivel global. Los niveles de cumplimiento suelen variar debido a factores como la conciencia normativa, la capacitación del personal, la disponibilidad de recursos y la implementación de medidas técnicas y organizativas.

En el contexto específico de Ecuador, las instituciones públicas pueden enfrentar desafíos para adaptarse y cumplir plenamente con la Ley Orgánica de Protección de Datos Personales. Algunas áreas críticas que podrían influir en el grado de cumplimiento incluyen:

1. Concientización y educación: La falta de conciencia sobre la importancia de la protección de datos y la legislación vigente puede afectar el cumplimiento. La educación continua del personal es esencial.
2. Recursos financieros y tecnológicos: La implementación de medidas de seguridad y el cumplimiento normativo a menudo requieren inversiones en tecnología y recursos humanos. Limitaciones financieras pueden afectar la capacidad de las instituciones para cumplir plenamente.
3. Procesos internos y políticas de privacidad: La falta de procesos internos claros y políticas de privacidad bien definidas puede dificultar la adecuación a los requisitos de la ley.

4. Supervisión y auditoría: La falta de supervisión continua y auditorías internas puede contribuir a un bajo grado de cumplimiento (Lucero, 2023), ya que la falta de monitoreo dificulta la identificación y corrección de posibles brechas.

Medidas de seguridad para la protección de datos personales.

La implementación de medidas de seguridad en instituciones públicas para la protección de datos personales suele ser un proceso complejo y multifacético. Estas medidas buscan garantizar la confidencialidad, integridad y disponibilidad de la información sensible, así como cumplir con los requisitos de la legislación de protección de datos. A continuación, se analizan algunas medidas en este contexto (ver tabla 2).

Tabla 2. Medidas generales de seguridad para la protección de datos personales.

No.	Medidas	Descripción
1	Políticas de privacidad y seguridad	Las instituciones públicas deben establecer políticas claras que aborden la privacidad y seguridad de los datos. Esto incluye la definición de roles y responsabilidades, así como la comunicación de las expectativas y obligaciones del personal.
2	Acceso autorizado y control de usuarios	Limitar el acceso a la información solo a aquellos empleados que lo necesitan para realizar sus funciones. Esto se logra a través de la asignación de roles y permisos específicos.
3	Cifrado de datos	La información sensible se cifra para protegerla en tránsito y durante el almacenamiento. Esto ayuda a prevenir accesos no autorizados, incluso en caso de brechas de seguridad.
4	Protección contra malware y virus	Instalación y actualización regular de software antivirus y antimalware para detectar y eliminar posibles amenazas.
5	Capacitación del personal	Brindar capacitación continua al personal sobre las mejores prácticas de seguridad y conciencia sobre amenazas (Zárate Zapata, 2021).
6	Auditorías y evaluaciones de seguridad	Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas e identificar posibles áreas de mejora.
7	Respuesta a incidentes	Desarrollar planes de respuesta a incidentes para abordar rápidamente cualquier violación de seguridad y minimizar el impacto.

Fuente: Elaboración propia.

La implementación efectiva de medidas de seguridad y principios de conservación en instituciones públicas de Babahoyo requiere una estrategia integral que abarque aspectos tecnológicos, culturales y legales. Identificar áreas de mejora en las prácticas de seguridad de la información es crucial para fortalecer la protección de datos en instituciones públicas, incluyendo el papel específico de las universidades. A continuación, se presentan los conjuntos de estrategias integrales específicas y prácticas, al considerar el contexto local (ver tabla 3).

Tabla 3. Conjuntos de estrategias integrales.

Cód.	Conjunto	Estrategia	Acciones
CE1	Infraestructura y tecnologías de seguridad	Actualización tecnológica	• Actualizar y fortalecer la infraestructura tecnológica. • Adoptar tecnologías avanzadas de seguridad. • Implementar técnicas de cifrado robustas.
		Gestión tecnológica eficiente:	• Establecer sistemas de gestión de identidad y control de acceso sólidos. • Desarrollar y compartir conocimientos sobre tecnologías emergentes.
CE2	Cultura organizacional y formación continua	Fomento de una cultura de seguridad	• Fomentar una cultura organizacional de seguridad de datos. • Ofrecer programas de formación y concientización.
		Capacitación continua	• Proporcionar formación continua sobre ciberseguridad y normativas de conservación. • Desarrollar programas académicos y cursos de formación especializada.
CE3	Normativas y adecuación legal:	Revisión y adecuación legal	• Revisar y ajustar las políticas y procedimientos para cumplir con la legislación vigente. • Contribuir con análisis legal y ético.
		Incentivos y certificaciones	• Establecer incentivos y programas de certificación para motivar el cumplimiento normativo. • Participar en la creación y evaluación de programas de certificación y reconocimiento.

CE4	Colaboración interinstitucional	Colaboración y compartir mejores prácticas	• Fomentar la colaboración entre instituciones para compartir información sobre amenazas y mejores prácticas. Facilitar la colaboración a través de eventos académicos y proyectos de investigación conjunta.
CE5	Investigación aplicada y desarrollo tecnológico	Investigación aplicada y desarrollo tecnológico	• Fomentar la investigación aplicada para desarrollar soluciones tecnológicas innovadoras. • Liderar proyectos de investigación en colaboración con instituciones y contribuir al desarrollo de tecnologías avanzadas.

Fuente: Elaboración propia.

Las estrategias propuestas pueden agruparse en cinco conjuntos fundamentales, cada uno centrado en aspectos específicos para fortalecer la seguridad y conservación de datos en instituciones públicas de Babahoyo.

A continuación, se propone criterios relevantes con sus pesos de importancia (ver tabla 4); luego se procede a la evaluación de los cinco conjuntos de estrategias integrales a partir de la modelación del método MOORA (ver tabla 5 a la 8).

Tabla 4. Criterios de evaluación.

Nº	**Criterio**	**Peso**
C1	Efectividad Tecnológica	0.3
C2	Impacto en la Cultura Organizacional	0.2
C3	Adecuación Legal y Normativa	0.2
C4	Capacidad de Colaboración Interinstitucional	0.1
C5	Contribución a la Investigación Aplicada	0.2

Fuente: Elaboración propia.

El método MOORA implica normalizar los valores y calcular la puntuación ponderada para cada conjunto de estrategias. Luego, se suma la puntuación ponderada para cada criterio.

Tabla 5. Matriz de decisión final.

Conjunto de Estrategias	C1	C2	C3	C4	C5
	Max	Max	Max	Max	Max
CE1	9	7	8	6	8
CE2	6	9	7	8	7
CE3	7	6	9	7	6
CE4	8	7	7	9	6
CE5	9	8	8	7	9
Suma de cuadrados	**311**	**279**	**307**	**279**	**266**
Raíz de cuadrados	**17.64**	**16.70**	**17.52**	**16.70**	**16.31**

Fuente: Elaboración propia.

Tabla 6. Matriz normalizada.

Conjunto de Estrategias	C1	C2	C3	C4	C5
	Max	Max	Max	Max	Max
CE1	0.510	0.419	0.457	0.359	0.491
CE2	0.340	0.539	0.400	0.479	0.429
CE3	0.397	0.359	0.514	0.419	0.368
CE4	0.454	0.419	0.400	0.539	0.368
CE5	0.510	0.479	0.457	0.419	0.552
w_j	**0.30**	**0.20**	**0.20**	**0.10**	**0.20**

Fuente: Elaboración propia.

Tabla 7. Matriz normalizada y ponderada.

Conjunto de Estrategias	C1	C2	C3	C4	C5
	Max	Max	Max	Max	Max
CE1	0.153	0.084	0.091	0.036	0.098
CE2	0.102	0.108	0.080	0.048	0.086
CE3	0.119	0.072	0.103	0.042	0.074
CE4	0.136	0.084	0.080	0.054	0.074
CE5	0.153	0.096	0.091	0.042	0.110
r_j	**0.153**	**0.108**	**0.103**	**0.054**	**0.110**

Fuente: Elaboración propia.

Tabla 8. Evaluación de cada alternativa por distancia a punto de referencia.

						Max	**Orden**
CE1	0.000	0.024	0.012	0.018	0.012	**0.024**	**2**
CE2	0.051	0.000	0.023	0.006	0.024	**0.051**	**4**
CE3	0.034	0.036	0.000	0.012	0.036	**0.036**	**3**
CE4	0.017	0.024	0.023	0.000	0.036	**0.036**	**3**
CE5	0.000	0.012	0.012	0.012	0.000	**0.012**	**1**

Fuente: Elaboración propia.

Una vez realizado el cálculo y análisis correspondiente, se determina como conjunto de estrategia integral de mayor prioridad según los criterios y pesos establecidos a la *investigación aplicada y desarrollo tecnológico* y como acciones a trabajar se encuentran:

- Fomentar la investigación aplicada para desarrollar soluciones tecnológicas innovadoras.
- Liderar proyectos de investigación en colaboración con instituciones y contribuir al desarrollo de tecnologías avanzadas.

Dentro de este conjunto, las estrategias relacionadas con la actualización tecnológica, la adopción de tecnologías avanzadas de seguridad, y la implementación de técnicas de cifrado robustas contribuyen directamente a establecer medidas ejecutivas concretas. Estas acciones fortalecen la infraestructura tecnológica, al asegurar que la administración pública pueda gestionar y tratar los datos personales de manera eficiente y segura.

Discusión.

Implementar tecnologías avanzadas, como sistemas de gestión de identidad y control de acceso (Solís et al., 2023), también forma parte de las medidas ejecutivas, ya que proporcionan la base para una administración segura y eficaz de la información. Estas estrategias técnicas son fundamentales para garantizar una gestión y tratamiento adecuados de los datos personales en el ámbito de la administración pública. A continuación, se proponen el desarrollo de la estrategia integral seleccionada

a partir de la implementación de proyectos claves en el fortalecimiento, seguridad y conservación de datos en instituciones públicas de Babahoyo (ver tabla 9).

Tabla 9. Proyectos claves en el fortalecimiento, seguridad y conservación de datos.

	Proyecto 1	**Proyecto 2**	**Proyecto 3**
Aspecto de Evaluación	**Fortalecimiento de la seguridad de datos en instituciones públicas mediante investigación en ciberseguridad.**	**Desarrollo de herramienta de gestión de identidad y acceso para instituciones públicas.**	**Estudio de prácticas y políticas de conservación de datos en instituciones públicas.**
Alcance	Mejora de la seguridad a través de ciberseguridad	Desarrollo de herramienta de gestión de identidad	Análisis y mejora de prácticas de conservación de datos
Tiempo	18 meses	24 meses	12 meses
Objetivo General	Mejora de la postura de seguridad de instituciones	Implementación de herramienta de gestión de identidad	Evaluar y mejorar prácticas de conservación de datos
Objetivos Específicos	Identificación de vulnerabilidades, Desarrollo de soluciones, Concienciación	Identificación de requisitos, Desarrollo de herramienta, Pruebas y ajustes	Análisis de políticas existentes, Evaluación de eficacia, Propuestas de mejora
Etapas	Investigación y análisis, Desarrollo, Implementación	Análisis de requisitos, Diseño y desarrollo, Pruebas y ajustes	Investigación de prácticas actuales, Evaluación de eficacia, Propuestas de mejora
Recursos	Personal de ciberseguridad, Equipos de laboratorio	Equipo de desarrollo de software, Expertos en gestión de identidad	Investigadores en protección de datos, Personal especializado en normativas de privacidad
Impacto Esperado	Mejora significativa en seguridad de datos	Mayor control de acceso, Reducción de riesgos	Desarrollo de políticas y prácticas más efectivas
Personal Calificado	Expertos en ciberseguridad, Personal docente	Ingenieros de software, Expertos en seguridad informática	Investigadores en protección de datos, Personal especializado en derecho digital
Niveles de Aprobación	Autoridades de instituciones y revisión ética	Autoridades de instituciones y revisión ética	Autoridades de instituciones y revisión ética
Financiamiento	Subvenciones, Fondos de investigación	Subvenciones, Fondos de investigación	Subvenciones, Fondos de investigación

	Proyecto 1	Proyecto 2	Proyecto 3
Aspecto de Evaluación	**Fortalecimiento de la seguridad de datos en instituciones públicas mediante investigación en ciberseguridad.**	**Desarrollo de herramienta de gestión de identidad y acceso para instituciones públicas.**	**Estudio de prácticas y políticas de conservación de datos en instituciones públicas.**
Resultados	Informe de vulnerabilidades, Soluciones implementadas, Materiales de concienciación	Herramienta implementada, Manuales de usuario	Informe de prácticas actuales, Propuestas de mejora
Beneficios Alcanzar	Mayor seguridad, Conocimiento avanzado en ciberseguridad, Establecimiento de buenas prácticas	Mayor control y seguridad en gestión de identidad, Eficiencia mejorada	Cumplimiento normativo mejorado, Desarrollo de estándares éticos

Fuente: Elaboración propia.

La implementación de los proyectos propuestos, permiten lograr avances significativos en la mejora de la seguridad y la gestión de datos en las instituciones públicas de Babahoyo. En el Proyecto 1, se identifican vulnerabilidades clave, y las soluciones desarrolladas no solo cierran las brechas, sino que también proporcionaron una conciencia más profunda sobre las amenazas cibernéticas (Abad & Arciniegas, 2023). Se evidencia un enfoque a la disminución en los incidentes de seguridad relacionados con la filtración de datos, lo que indica un fortalecimiento en las defensas digitales.

El Proyecto 2, se centra en la gestión de identidad y acceso, al permitir la implementación eficaz de herramientas personalizadas en un control de acceso más riguroso y una reducción sustancial de los riesgos asociados con el acceso no autorizado. La aplicación de este proyecto permite a las instituciones públicas experimentar una transición más suave hacia un entorno digital seguro, y la eficiencia en la administración de datos significativamente. La herramienta propuesta permite integrar de manera efectiva en los procesos existentes, al demostrar la adaptabilidad y utilidad práctica.

En el Proyecto 3, se analiza y mejoran las prácticas de conservación de datos (De la Rosa-Martín & León-González, 2023), al revelar un cambio positivo en la cultura y manejo de la información en las instituciones. Se enfoca en la implementación de políticas y prácticas más éticas y eficaces; de modo,

que asegure un mayor cumplimiento normativo y una mayor confianza del público en la gestión de datos por parte de las instituciones públicas; además, fomenta la colaboración entre las instituciones y las universidades en la implementación de las mejoras.

Los resultados destacan la importancia de abordar la seguridad y la conservación de datos de manera integral. La combinación de proyectos especializados en ciberseguridad, gestión de identidad y acceso, y prácticas de conservación demostró ser efectiva para fortalecer la postura general de las instituciones públicas de Babahoyo. La sinergia entre estas iniciativas permitió un enfoque holístico, al abordar diferentes aspectos de la protección de datos.

La experiencia de Babahoyo puede servir como modelo para otras ciudades y regiones que buscan mejorar la seguridad y la conservación de datos en entornos institucionales. Las lecciones aprendidas destacan la necesidad de una adaptabilidad continua y la importancia de la colaboración interdisciplinaria para abordar los desafíos en constante evolución en el ámbito de la protección de datos.

CONCLUSIONES.

Se concluye que:

- La implementación exitosa de medidas de seguridad y principios de conservación de datos en instituciones públicas de Babahoyo destaca la importancia de un enfoque holístico. La combinación de estrategias específicas, como la ciberseguridad, gestión de identidad y prácticas de conservación, demostró ser más efectiva que abordar cada aspecto por separado. La sinergia entre estas áreas aseguró una mejora integral en la protección de datos, al fortalecer la postura de seguridad de manera significativa.
- La participación activa de las universidades desempeñó un papel crucial en el éxito de las iniciativas. La colaboración entre académicos, estudiantes y profesionales de las instituciones públicas permitió aprovechar el conocimiento especializado en diversas disciplinas, desde ciberseguridad hasta

derecho digital. Esta sinergia fomentó un entorno de investigación aplicada y desarrollo tecnológico, al enriquecer la implementación de estrategias y promover la conexión entre la teoría y la práctica.

- La aplicación del método MOORA para evaluar y comparar los conjuntos de estrategias propuestos proporcionó una validación objetiva de la elección de la estrategia integral a la "investigación aplicada y desarrollo tecnológico". El método MOORA destacó la superioridad de esta estrategia al asignar pesos a criterios relevantes, como el cumplimiento normativo, la oportunidad de medidas de seguridad, la notificación de incidentes y la gestión efectiva de datos; de modo, que los resultados objetivos refuerzan la elección de enfoques que tienen un impacto más directo y significativo en la seguridad y conservación de datos.

REFERENCIAS BIBLIOGRÁFICAS.

1. Cornejo, A., & Sánchez, D. (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. Código Científico Revista de Investigación, 4(E2), 984-1023. http://revistacodigocientifico.itslosandes.net/index.php/1/article/view/192
2. De la Rosa-Martín, T., & León-González, J. L. (2023). Diseño del sistema automatizado para la generación y gestión de documentos en la etapa precontractual de compras públicas para instituciones públicas en el Ecuador. Revista Transdiciplinaria de Estudios Sociales y Tecnológicos, 3(1), 14-25. https://revista.excedinter.com/index.php/rtest/article/view/60
3. Grau, A. B. (2019). El papel de la negociación colectiva en la ley de protección de datos personales y garantía de derechos digitales en España. Labour & Law Issues, 5(1), 1-14. https://labourlaw.unibo.it/article/view/9608
4. Hasan Hakan, B., & İsmail, T. (2022). Investigation of offshore wind characteristics for the northwest of Türkiye region by using multi-criteria decision-making method (MOORA). Results in engineering, 16(December), 100757-100757. https://www.sciencedirect.com/science/article/pii/S2590123022004273

5. Rovira, Z., Robles, L., & Castillo, J. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. Polo del Conocimiento, 8(8), 1355-1373. https://polodelconocimiento.com/ojs/index.php/es/article/view/5908
6. Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. Technology Rain Journal, 2(2), e17-e17. http://technologyrain.com.ar/index.php/trj/article/view/17
7. Minaya, M., Minaya, R., Intriago, M., & Intriago, J. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5(4), 584-599. http://www.editorialalema.org/index.php/pentaciencias/article/view/700
8. Abad, K., & Arciniegas, C. (2023). La inteligencia artificial y la limitación al derecho a la privacidad cibernética, en estudiantes de Jurisprudencia, Cuenca-Ecuador 2022: Artificial intelligence and the limitation of the right to cybernetic privacy, in students of Jurisprudence, Cuenca-Ecuador 2022. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 4(1), 657-666. http://latam.redilat.org/index.php/lt/article/view/284
9. Patnaik, P. K., Swain, P. T. R., Mishra, S. K., Purohit, A., & Biswas, S. (2020). Composite material selection for structural applications based on AHP-MOORA approach. Materials Today: Proceedings, 33(Part 8), 5659-5663. https://www.sciencedirect.com/science/article/abs/pii/S221478532032678X
10. Pesantez-Maura, T. K., & Torres-Ortuño, I. D. (2023). Cancelación, supresión y olvido en el marco de la protección de datos personales en el Ecuador. MQRInvestigar, 7(2), 1001-1016. http://www.investigarmqr.com/ojs/index.php/mqr/article/view/385

11. Rivera, Y., & Maldonado, L. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. Polo del Conocimiento, 8(10), 982-1009. https://polodelconocimiento.com/ojs/index.php/es/article/view/6172#google_vignette
12. Durán, M. & Zamora, A. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. MQRInvestigar, 7(1), 330-343. http://www.investigarmqr.com/ojs/index.php/mqr/article/view/170
13. Solís, G., Valderrama, C., Tejedor, E., & de, V. (2023). Seguridad de los Sistemas Informáticos Universitarios: : Retos Pendientes. REICIT, 2(2), 113-142. https://uptv.up.ac.pa/index.php/REICIT/article/view/3585
14. Cevallos, L., & Delgado, J. (2023). Ley de Protección de Datos Personales: Impacto en la promoción del ODS 16 en el Ecuador. Reincisol., 2(4), 271-303. http://www.reincisol.com/ojs/index.php/reincisol/article/view/61
15. Zárate Zapata, G. H. (2021). LAS NUEVAS AMENAZAS A LA SEGURIDAD EN EL CONTEXTO LATINOAMERICANO. Revista de la Academia del Guerra del Ejército Ecuatoriano, 14(1), 8. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/VOL14ART3

DATOS DE LOS AUTORES.

1. **Nelly Valeria Vinueza Ochoa.** Magister en Derecho Constitucional. Docente de la Universidad Regional Autónoma de Los Andes, Sede Babahoyo, Ecuador. E-mail: ub.nellyvinueza@uniandes.edu.ec
2. **Miguel Ángel Macías Álvarez.** Estudiante de la Universidad Regional Autónoma de Los Andes, Sede Babahoyo, Ecuador. E-mail: db.miguelama56@uniandes.edu.ec

3. **Rosa Leonor Maldonado Manzano.** Magister en Derecho de Familia Mención en Mediación y Arbitraje Familiar. Docente de la Universidad Regional Autónoma de Los Andes, Sede Babahoyo, Ecuador. E-mail: ub.c.derecho@uniandes.edu.ec

RECIBIDO: 5 de septiembre del 2023. **APROBADO:** 13 de octubre del 2023.