IDEAS

Innovation & Development in Engineering and Applied Science

Journal homepage:
https://revistasojs.utn.edu.ec/index.php/ideas

Evaluación de la madurez de la gobernanza de tecnologías de la información en un GAD rural ecuatoriano mediante COBIT 2019

Evaluation of the Maturity of Information Technology Governance in an Ecuadorian Rural Decentralised Autonomous Government Using COBIT 2019

Jenny Iñiguez[a], Marco Pusdá[a]

[a] Universidad Técnica del Norte, Ecuador.

Recibido: 2025-07-21, Aceptado: 2026-05-07, Publicado: 2026-06-30
Autor de correspondencia:
Jenny Iñiguez: *jpiniguezz@utn.edu.ec*
DOI: https://doi.org/10.53358/ideas.v8i2.1314

PALABRAS CLAVES:
Gobernanza de TI; Seguridad informática; COBIT 2019; PILAR.

RESUMEN
Las instituciones públicas enfrentan desafíos significativos para garantizar una gobernanza efectiva de las Tecnologías de la Información (TI), esencial para la eficiencia institucional. Este estudio tiene como objetivo proponer y validar un modelo metodológico basado en COBIT 2019 para medir y mejorar la madurez de los procesos de TI en el GAD Parroquial Rural de Tufiño. La metodología empleada fue de enfoque mixto y se estructuró en cinco fases: diagnóstico institucional, recolección de datos, evaluación de madurez, aplicación de factores de diseño y validación de propuestas. Los resultados fueron validados mediante la metodología Delphi en dos rondas con diez expertos. Los hallazgos indican un nivel inicial de madurez de 0,6, evidenciando brechas significativas respecto al nivel objetivo de 2,4. La propuesta de mejora fue validada en dos rondas Delphi con índices de aceptación del 92 % y 100 %. El modelo combinado de COBIT 2019 y la metodología Delphi permitió evaluar la efectividad de COBIT 2019 para fortalecer la gobernanza de TI en el GADP-Tufiño. Su aplicación resultó efectiva y replicable en instituciones públicas y privadas.

KEYWORDS:
IT governance; Information security; COBIT 2019; PILAR.

ABSTRACT
Public institutions face significant challenges in ensuring adequate Information Technology (IT) governance, which is essential for institutional efficiency. This study aimed to propose and validate a methodological model based on COBIT 2019 to measure and improve the maturity of IT processes in the Rural Parish Decentralised Autonomous Government of Tufiño. The methodology employed followed a mixed-methods approach structured into five phases: institutional diagnosis, data collection, maturity assessment, application of design factors, and validation of improvement proposals. The results were validated through the Delphi method in two rounds with ten experts. The findings indicate an initial maturity level of 0.6, revealing significant gaps in relation to the target level of 2.4. The improvement proposal was validated in two Delphi rounds, achieving acceptance rates of 92 % and 100 %.The combined model of COBIT 2019 and the Delphi method made it possible to evaluate the effectiveness of COBIT 2019 in strengthening IT governance in GADP-Tufiño. Its application proved to be effective and replicable in both public and private institutions.

Cómo citar

Evaluación De La Madurez De La Gobernanza De Tecnologías De La Información en un GAD Rural Ecuatoriano Mediante COBIT 2019. (s. f.). *Innovation & Development in Engineering and Applied Science*, *8*(2), 13.
https://doi.org/10.53358/ideas.v8i2.1314

1. Introducción

La transformación digital de las organizaciones públicas plantea el reto de gestionar eficientemente las tecnologías de información, garantizando su alineación con los objetivos institucionales. El marco COBIT 2019 [1], proporciona una estructura integral para evaluar mejorar la gobernanza de TI, siendo especialmente útil en instituciones con limitaciones presupuestarias estructurales, diversos estudios han abordado la implementación del marco COBIT 2019 en organizaciones públicas y privadas con el objetivo de mejorar la gobernanza de las Tecnologías de la Información, desempeñando un papel esencial en la creación de planes de seguridad informática, proporcionando un enfoque personalizado para las necesidades particulares de cada institución y facilitando la identificación y manejo de riesgos.

En concordancia con el artículo 4.2.2 de la Transparencia y acceso a la información pública [2], se destaca la importancia de garantizar la integridad, accesibilidad y confidencialidad de la información en el contexto institucional. El Plan de Desarrollo para el Nuevo Ecuador 2024-2025, mediante la política 3.12 [3], establece como objetivo fortalecer la ciberseguridad en telecomunicaciones, implementando estrategias que protejan los datos y la infraestructura digital del país.

Tipán [4] se propuso un modelo de ciberseguridad basado en COBIT 2019 y NIST para la empresa pública CNT. La metodología incluyó entrevistas, análisis documental y validación Delphi, diseñando un sistema de control de riesgos y lineamientos de gobernanza que mejoraron la gestión de TI en un 35 %, aumentando la madurez de $2{,}1$ a $3{,}4$ y logrando un 93 % de aceptación.

En el trabajo de Cortés [5], se evaluó la implementación de COBIT 2019 en la Municipalidad de Carrillo, Costa Rica, mediante auditorías internas y matrices de madurez. Se plantearon acciones correctivas en los dominios APO y DSS, aumentando el cumplimiento del 68 % al 87 % y la madurez de $2{,}3$ a $3{,}1$.

Por su parte, Alvarado y Andrade [6] propusieron un modelo de gobierno de TI basado en COBIT 2019 para una institución educativa pública, centrado en procesos críticos como APO01, APO07, BAI01, BAI03, DSS01, DSS05 y MEA01. En este estudio, se identificó un nivel inicial de $1{,}58$ y se planteó un plan de mejora proyectando niveles entre $2{,}5$ y $3{,}0$, con un aumento esperado del 45 % en cumplimiento, destacando la importancia del talento humano y la evaluación continua.

En la investigación de Lompoliu [7] se reportó una reducción del 40 % en incidentes de seguridad y un 98 % de aceptación institucional. El modelo planteado por Abdullah y Mustofa [8] analizó la aplicación de COBIT 2019 en el Ministerio de Educación y Cultura de Indonesia, concluyendo que fortaleció la toma de decisiones, elevando la madurez de $2{,}2$ a $3{,}3$ y la efectividad en un 27 %.Según Jaime y Barata [9] se realizó un mapeo entre herramientas FLOSS y los objetivos de COBIT 2019, mejorando la gobernanza de TI en entidades públicas, reduciendo costes operativos en un 30 %, alcanzando un nivel de madurez de $3{,}0$ y cubriendo el 75 % de los objetivos.

En la propuesta de Jennifer Felicia [10] auditó la implementación de software contable en escuelas secundarias de Yakarta usando COBIT 2019. La madurez promedio fue baja ($1-2$, media $1{,}4$) frente al nivel esperado 5, con una brecha superior al 70 % y recomendaciones específicas por dominio.

Carlos Prasca y Adriana Suárez [11] diseñaron un modelo de gobernanza para la Gobernación del Atlántico alineado con COBIT 2019 y la política de Gobierno Digital. Los procesos clave tenían niveles entre $0{,}7$ y $1{,}2$, proponiendo un plan para alcanzar niveles $2-3$ en dos años. Yohanes Beato y Ditdit Nugeraha [12] evaluaron la continuidad del negocio en instituciones públicas con COBIT 2019 (DSS04), encontrando madurez parcial en nivel 1, con solo el 30 % de salvaguardas implementadas y una brecha significativa para alcanzar nivel 3.

Según Jose Torregroza [13] destacó que las pequeñas organizaciones suelen partir de niveles bajos ($0-1$) y, con prácticas recomendadas, pueden avanzar a niveles $2-3$ para maximizar recursos tecnológicos. Fitriyani y Muhammad [14] concluyeron que COBIT 2019 es efectivo en instituciones educativas con recursos limitados como la Universidad Estatal de Malang, aumentando la madurez de $1{,}9$ a $3{,}2$ y alcanzando un 96 % de aceptación. En el estudio de Ramadhani [15] se encontró que COBIT 2019 permitió a BTS.id optimizar áreas críticas, elevando el cumplimiento en un 22 % y la gestión de riesgos al 90 %. Por último, Rizky [16] evaluó la gobernanza en SMK Negeri 4 Malang (DSS02), identificando nivel 2 y proyectando nivel 3 en 12 meses, con mejoras del 18 % en tiempos de respuesta y 25 % en satisfacción.

En el caso específico del GADP-Tufiño, enfrenta riesgos en la protección de su información, activos e infraestructura tecnológica. Carece de una estructura adecuada y de políticas claras para gestionar sus activos tecnológicos, como servidores, sistemas de acceso y equipos de red. En la evaluación de madurez de los procesos clave mediante COBIT 2019 se utilizaron dominios como APO01 gestionar el marco de gobierno, APO03 gestionar la arquitectura empresarial, APO12 gestionar los riesgos de TI, APO13 gestionar la seguridad, DSS05 gestionar la seguridad de los servicios [17]. Frente a este panorama, se emplea el marco COBIT 2019 a través de los Factores de Diseño (DF), los cuales permiten estructurar el sistema de gobernanza de una organización [18].

COBIT 2019 define once (DF) [19] que influyen directamente en cómo debe ser diseñado un sistema de gobierno de TI para una organización y establece el Nivel Objetivo Sugerido de Capacidad de Procesos (NOSCP), como se muestra en la Tabla 1.

Tabla 1: (NOSCP)

Proceso COBIT	NOSCP
APO001	2
APO003	1
APO012	2
APO013	4
DSS06	3

Este estudio se enfoca en el GADP-Tufiño, una entidad con infraestructura limitada y carente de políticas formales de seguridad informática, mediante la evaluación de la madurez de los procesos clave. El objetivo general es diagnosticar y proponer un modelo metodológico replicable para medir y fortalecer la madurez de los procesos de TI mediante COBIT 2019 [17], validando las acciones mediante el método Delphi.

2. Materiales y Métodos

Se adoptó un enfoque cualitativo-descriptivo con componentes cuantitativos para evaluar la madurez en seguridad informática, el análisis documental y la observación directa permitieron explorar políticas y prácticas institucionales, mientras que la encuesta estructurada al personal del GADP-Tufiño cuantificaron la percepción sobre la eficacia de los controles y la alineación de los procesos de TI.

La metodología se organizó en cinco fases secuenciales, representadas en la figura 1, y se fundamentó en el marco de referencia COBIT 2019, reconocido por sus lineamientos estructurados para la gobernanza y gestión de tecnologías de información.

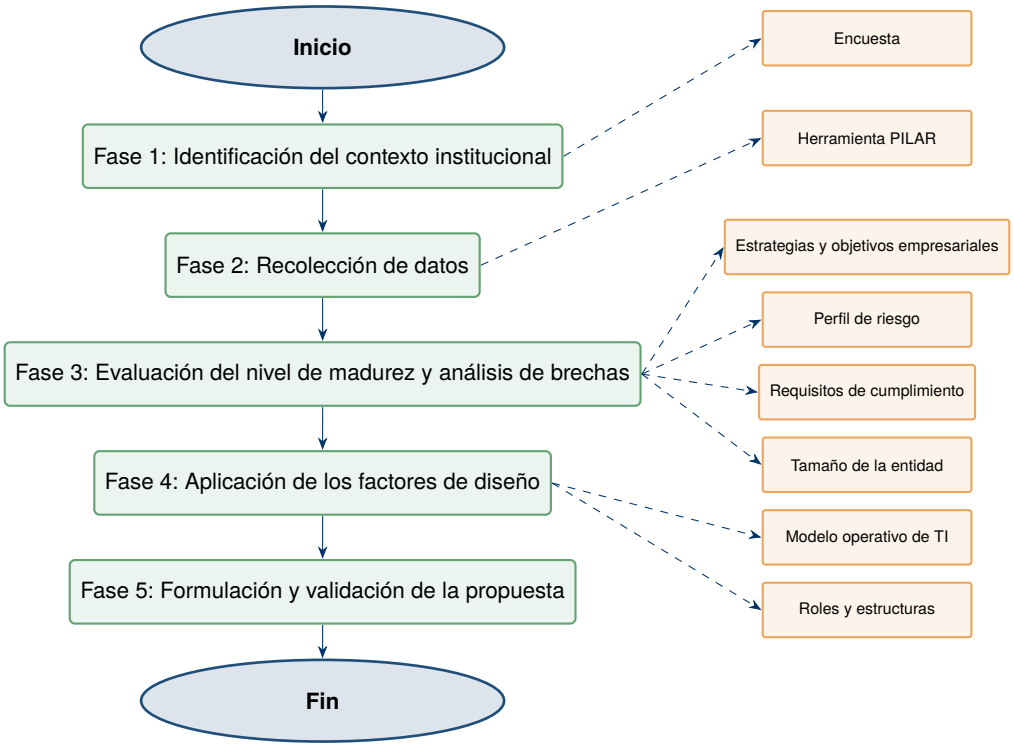

Fig. 1: Fases secuenciales del proceso metodológico fundamentadas en el marco COBIT 2019. Autoría propia.

Fase 1: Identificación del contexto institucional

Se inició con el análisis del entorno operativo del GADP-Tufiño, recopilando información sobre su estructura organizacional, recursos tecnológicos disponibles y nivel de formalización de procesos de TI, para ello, se aplicó una encuesta al personal técnico y administrativo, con el propósito de identificar el nivel de conocimiento en aspectos relacionados con seguridad informática y gobernanza tecnológica.

fase 2: Recolección de datos

Se utilizó una combinación de observación directa, encuestas semiestructuradas donde se realizó un formulario en google forms compuesta por 15 preguntas alineadas a los dominios APO y DSS seleccionados y se realizó la revisión documental para identificar la existencia de políticas o manuales de seguridad.

Se utilizó la herramienta PILAR, orientada al análisis de riesgos, la cual es una aplicación de carácter privativo, para identificar activos críticos, amenazas, controles existentes y carencias en la infraestructura tecnológica, el análisis se realizó mediante una versión de prueba de la herramienta, lo que permitió obtener información relevante que fue contrastada con los objetivos estratégicos institucionales y los requerimientos operativos del GADP-Tufiño.

Fase 3: Evaluación de madurez y análisis de brechas

Con base en los datos recopilados, se aplicó la escala de madurez del modelo COBIT 2019 a cinco dominios clave: APO01, APO03, APO12, APO13 y DSS05. Para cada dominio, se evaluaron las prácticas existentes frente al modelo de capacidad, que abarca los niveles desde 0 (inexistente) hasta 5 (optimizado).

A partir de esta evaluación se determinaron las brechas entre el estado actual y el Nivel de Capacidad Objetivo (NCO) deseado, como se muestra en la Tabla 2.

fase 4: Aplicación de factores de diseño

Se analizaron los (DF), establecidos por COBIT 2019, incluyendo: perfil de riesgos, tamaño de la entidad, modelo operativo de TI, requisitos de cumplimiento normativo, estructuras organizativas y objetivos institucionales, esta fase permitió personalizar las recomendaciones de mejora y asegurar su viabilidad de implementación.

Por lo tanto, se justifica la selección de los procesos APO01, APO03, APO12, APO13 y DSS05 como ejes prioritarios para fortalecer la gobernanza de las tecnologías de la información dentro del GADP-Tufiño, como se muestra en la Tabla 3.

Tabla 2: Niveles de madurez en COBIT 2019 (modelo de capacidad)

Nivel	**Descripción**
0 - Incompleto	El proceso no alcanza su propósito ni está implementado.
1 - Realizado	El proceso se ejecuta, pero sin control formal ni consistencia.
2 - Gestionado	El proceso está planificado, monitoreado y ajustado cuando es necesario.
3 - Establecido	El proceso sigue procedimientos documentados y se implementa consistentemente.
4 - Predecible	El proceso se mide y es capaz de alcanzar resultados esperados con estabilidad.
5 - Optimizado	El proceso se mejora continuamente basado en datos y análisis de desempeño.

Tabla 3: Factores de diseño evaluados por proceso COBIT 2019

Proceso COBIT	**Factores de diseño evaluados**
APO01	DF1, DF2, DF7, DF11
APO03	DF1, DF4, DF7
APO12	DF2, DF3, DF5, DF6
APO13	DF4, DF5, DF6
DSS05	DF3, DF4, DF5, DF6

Para determinar el nivel de madurez de los procesos de seguridad informática del GADP-Tufiño, se aplicaron los dominios APO01, APO03, APO12, APO13 y DSS05 del marco COBIT 2019, analizando cada uno mediante técnicas estadísticas descriptivas como el promedio, desviación estándar.

Inicialmente, se obtuvo el promedio de los resultados de la encuesta realizada al personal clave, con el fin de identificar la consistencia y dispersión de los datos. En la figura 2, se representan los valores obtenidos, considerando el nivel promedio de madurez en el rango de 0 a 5, correspondiente al (Modelo de Capacidad).

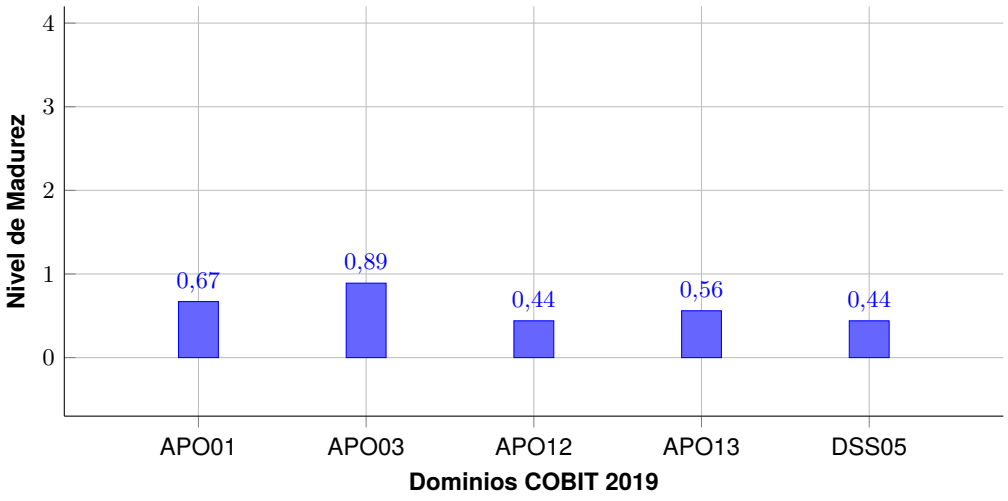

Fig. 2: Evaluación del nivel de madurez por dominio según COBIT 2019

Los resultados son bajos, ya que ningún dominio alcanza el nivel mínimo (1 Realizado). Se consideró el uso de (DF), que implica analizar la situación actual de la organización considerando aspectos clave como la estrategia empresarial y los riesgos tecnológicos, como se muestra en la figura 3, al aplicar (DF) en el marco COBIT 2019, como complemento a los dominios APO01, APO03, AP012, APO13, DSS05, lo que permitió la implementación del sistema de gobernanza personalizado y adecuado a las necesidades y capacidades del entorno institucional.

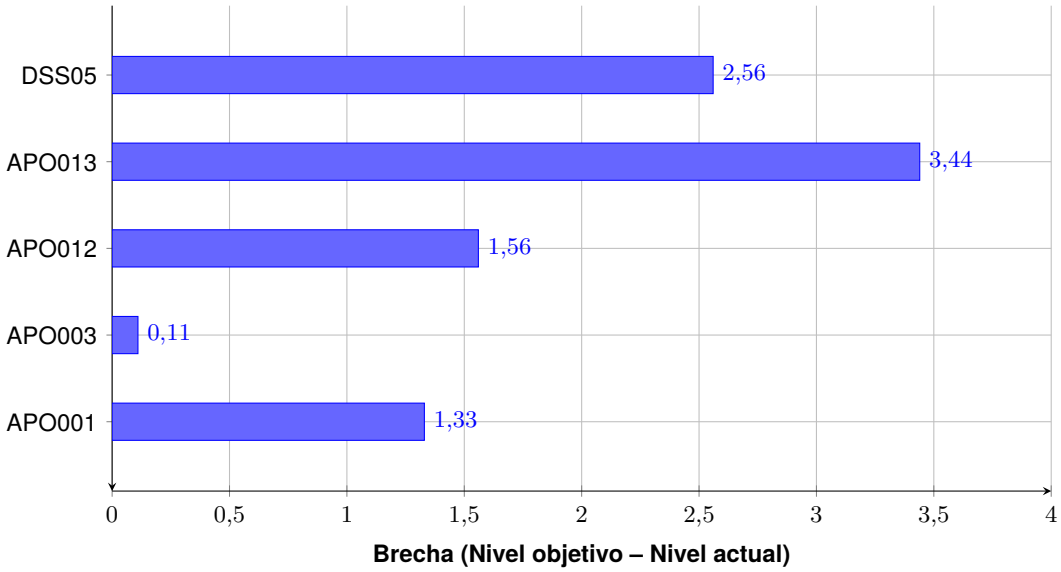

Fig. 3: Comparación de la brecha entre el nivel objetivo y el nivel actual por proceso COBIT

Para caracterizar cuantitativamente el estado de los procesos evaluados, se calcularon indicadores estadísticos clave que permiten comprender tanto el nivel actual como las aspiraciones de madurez institucional. Entre estos se incluyen la media de la madurez promedio (MMP), la desviación estándar (DE), la media del nivel objetivo (MNO) y la media de la brecha (MB), estos valores facilitan identificar las debilidades actuales, la consistencia entre procesos y el esfuerzo requerido para alcanzar los objetivos establecidos.

La media de la madurez promedio se calcula según la ecuación (1).

$$\bar{x} = \frac{\sum \text{madurez}}{n} \tag{1}$$

El valor obtenido para la MMP fue 0,60, este valor representa el estado actual de madurez de los procesos evaluados, que sugiere que los procesos apenas se están ejecutando.

La desviación estándar se calcula según la Ecuación (2).

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2} \tag{2}$$

El valor obtenido de la desviación estándar fue 0,60, un valor que implica que hay cierta variabilidad, pero que la mayoría de los procesos evaluados están igualmente bajos.

Media del Nivel Objetivo

$$MNO = \frac{2+1+2+4+3}{5} = \frac{12}{5} = 2,4$$

El valor de 2,4 indica que la organización aspira a que sus procesos estén definidos y gestionados.

Media de la Brecha (MB)

$$MB - NO - NP = \frac{1,33+0,11+1,56+3,44+2,56}{5} = \frac{9}{5} = 1,8$$

Una brecha de 1,8 puntos es significativa, y señala que la organización necesita escalar al menos dos niveles de madurez por proceso.

La figura 4 muestra una comparación gráfica de los valores clave según el marco COBIT 2019.

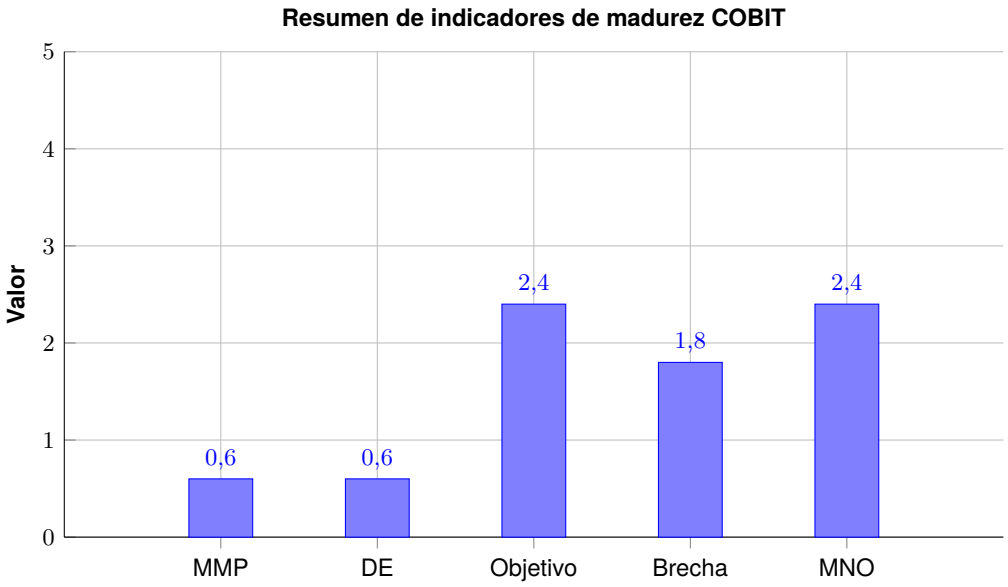

Fig. 4: Comparación de indicadores clave: madurez promedio, desviación estándar, nivel objetivo y brecha

El uso de la herramienta PILAR permitió identificar las brechas en la infraestructura tecnológica, además de establecer un diagnóstico inicial del nivel de madurez en la implementación de controles de seguridad. También permitió identificar los controles que requieren fortalecimiento y priorizar acciones según la exposición al riesgo, el cumplimiento normativo y la criticidad de los servicios tecnológicos evaluados. El significado de los niveles L0 a L5 de la aplicación PILAR se muestra en la Tabla 4.

Tabla 4: Significado de los niveles L0 a L5 de la aplicación PILAR

Nivel	Descripción	Interpretación práctica
L0	Inexistente	No existe ningún tipo de control implementado.
L1	Implementación mínima	El control existe de forma informal o parcial.
L2	Implementación básica	El control está documentado y parcialmente aplicado.
L3	Implementación completa	El control está completamente implementado y se encuentra en operación.
L4	Gestión activa	El control es monitoreado y revisado regularmente.
L5	Optimización y mejora continua	El control se mejora continuamente mediante métricas y análisis.

Cada fila representa una salvaguarda (control de seguridad).
Nivel actual (current) → qué tan implementada está.
Nivel objetivo (target) → meta recomendada.
Nivel de PILAR sugerido → en algunos casos aparece “L2-L5”.

Como parte del análisis, la Tabla 5 muestra la evaluación del nivel de implementación de las salvaguardas.

Tabla 5: Evaluación de salvaguardas: situación actual y niveles objetivo

Aspecto	TDP	Rec.	Salvaguarda	Current	Target
G	EL	5	Identificación y autenticación [IA]	-L1	L2-L5
T	EL	4	Control de acceso lógico [AC]	-L1	L2-L4

Continúa en la siguiente página

Tabla 5 (continuación)

Aspecto	TDP	Rec.	Salvaguarda	Current	Target
G	PR	4	Protección de la Información [INF]	-L1	L2-L4
T	EL	4	Protección de claves criptográficas [SC-12]	L0	L2-L3
G	PR	5	[PE] Protección física de los equipos	L1	L3
G	CR	5	[IM] Gestión de incidentes	-L1	L2-L3
F	EL	8	[tools] Herramientas de seguridad	-L1	L2-L3
G	CR	5	[VR] Gestión de vulnerabilidades	—	L2-L3
G	AD	3	[NEW] Adquisición / desarrollo	-L1	L2-L3
G	PR	3	[PPS] Protección del perímetro físico	-L1	L3

Los resultados de las salvaguardas muestran niveles de -L1 o L0, lo que denota un estado de no implementación. La comparación entre los niveles actuales identificados y el nivel deseado (L3) evidencia brechas que indican debilidades en la implementación o la ausencia de controles, como se puede observar en la figura 5.

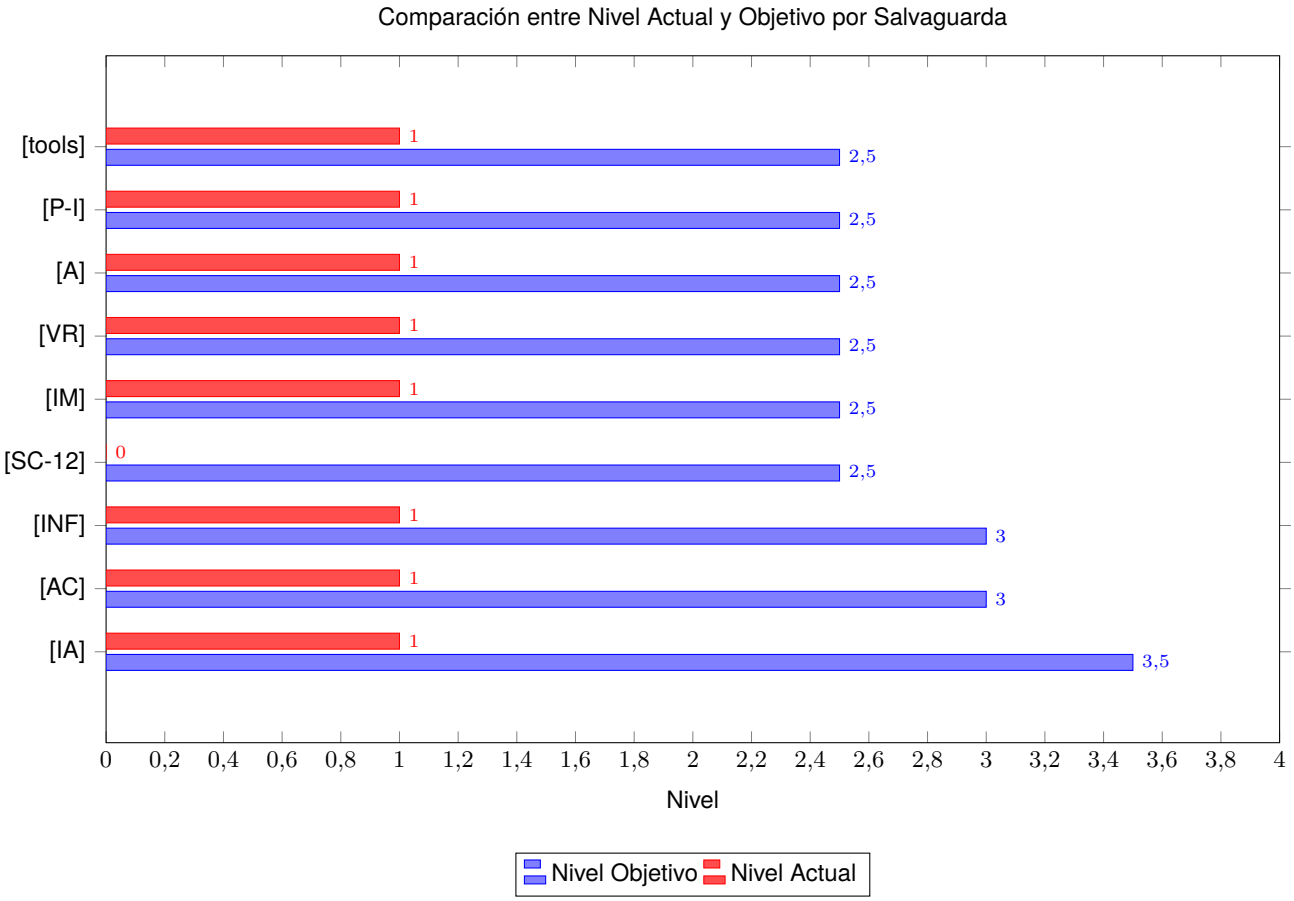

Fig. 5: Comparación entre nivel actual y objetivo por salvaguarda. Autor propio.

Fase 5: Formulación y validación de la propuesta

A partir del diagnóstico y del análisis de brechas, se diseñó una propuesta de mejora que incluyó controles técnicos y administrativos; las acciones sugeridas abarcaron la implementación y creación de políticas de seguridad y campañas de concienciación institucional. La propuesta fue evaluada mediante el método Delphi en dos rondas, con la participación de diez expertos en ciberseguridad y gobernanza de TI con experiencia en el sector público y privado, se empleó una escala Likert de cinco niveles para determinar el grado de madurez.

En la primera ronda se recolectaron respuestas individuales mediante una matriz estructurada. Los expertos evaluaron los dominios APO01, APO03, APO12, APO13 y DSS05, emitiendo observaciones como la implementación de una política para auditoría interna y mejora continua (MEA01), que está directamente relacionada con documentar, avaluar y monitorear los controles de seguridad y el seguimiento para fortalecer políticas específicas, como respaldo de datos, definición de roles de gobernanza y gestión de incidentes.

En la figura 6 se observa qué políticas tienen bajo desempeño y cuáles presentan alta dispersión, lo que indica desacuerdo entre evaluadores o implementación inconsistente. A partir de sus sugerencias se realizaron ajustes en el documento de políticas y se clarificaron los criterios de evaluación.

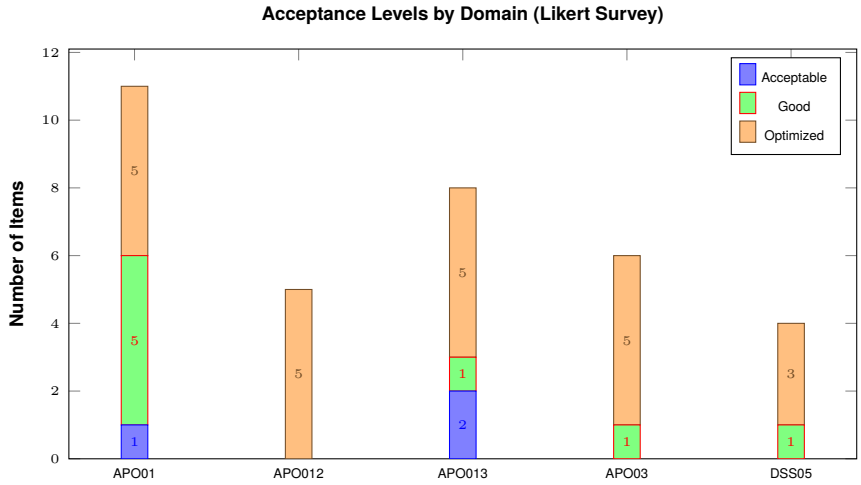

Fig. 6: Acceptance Levels by Domain in Likert-Type Survey

El entorno evaluado en la Tabla 6 muestra una implementación madura de los procesos de gobernanza y gestión de TI, sin registros de debilidades significativas (niveles Aceptables). Los dominios DSS05 y APO12 lideran en cuanto a desempeño optimizado, mientras que APO1,APO03 y APO013 requieren atención específica para escalar sus buenas prácticas al siguiente nivel. En conjunto, estos resultados respaldan un entorno de TI bien gestionado y seguro, alineado con buenas prácticas internacionales.

Tabla 6: Madurez Promedio por dominio

Dominio	**Promedio**
APO01	4,49
APO012	4,74
APO013	4,49
APO03	4,58
DSS05	4,68

El cálculo del Índice de Aceptación se obtuvo a partir del promedio real general (4,60), según la siguiente expresión (3):

$$\text{Índice de Aceptación} = \frac{4{,}60}{5} \cdot 100 = 92\,\% \tag{3}$$

Este valor indica el porcentaje de aceptación respecto a la escala máxima, el índice global de aceptación es del 92 %, lo cual representa un nivel favorable en la escala de 5 puntos. Esto refleja que la percepción de cumplimiento o madurez en los dominios evaluados está en el nivel optimizado. En la segunda ronda, se aplicó el instrumento con las correcciones de la primera ronda, no se registraron nuevas observaciones ni cambios significativos en las puntuaciones, alcanzando el nivel de madurez esperado y una validación metodológica exitosa, figura 7. Se puede evidenciar una mejora significativa en la segunda ronda, demostrando que las sugerencias fueron implementadas exitosamente y que se alcanzó un alto nivel de acuerdo entre los evaluadores.

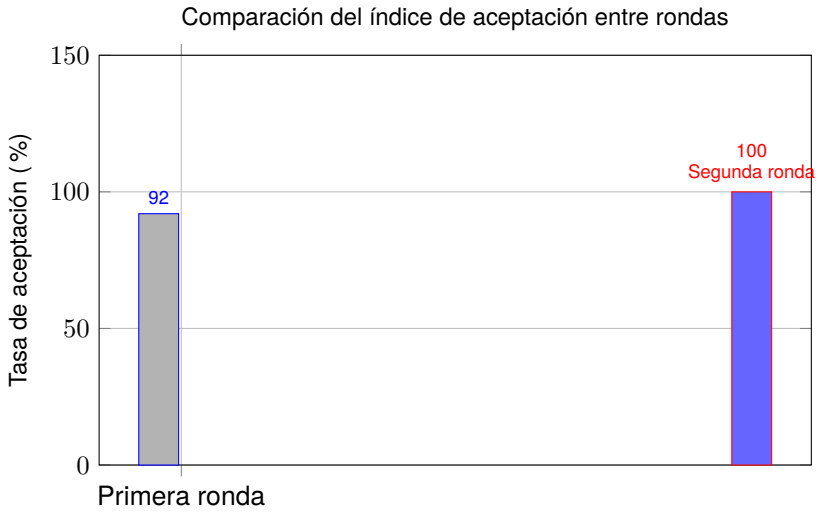

Fig. 7: Índice de aceptación

La selección de COBIT 2019 respondió a su enfoque integral y adaptable, ideal para instituciones pequeñas con necesidades concretas de gobernanza de TI, su estructura permite evaluar la madurez, definir brechas y personalizar soluciones mediante factores de diseño [17].La metodología DELPHI fue adecuada para validar la propuesta con expertos de forma estructurada y anónima, como se recomienda en contextos donde se requiere consenso técnico [12].

La herramienta PILAR es de acceso gratuito por 30 días, lo que la hace viable para gobiernos locales con recursos limitados [20], y permitió evaluar amenazas y vulnerabilidades, integrando un enfoque técnico accesible y coherente con los principios de COBIT 2019.

La Tabla 7 presenta un resumen de los procesos COBIT 2019 priorizados, detallando el nivel inicial de madurez, las acciones de mejora propuestas y el nivel de madurez esperado para cada dominio. Estas acciones se definieron a partir del análisis integrado de la evaluación de salvaguardas mediante la herramienta PILAR, el escaneo de vulnerabilidades externas y los resultados de la encuesta institucional, los cuales evidenciaron debilidades significativas en gobernanza, arquitectura empresarial, gestión de riesgos, seguridad de la información y gestión de incidentes. La implementación de estas políticas permite establecer una hoja de ruta estructurada para el fortalecimiento progresivo de la seguridad informática y la gobernanza de TI en el GADP-Tufiño.

Tabla 7: Resumen de procesos COBIT 2019: nivel inicial, acciones de mejora y nivel esperado

Proceso	Nivel inicial	Acción de mejora propuesta	Nivel esperado
APO01	0,67	Definir y formalizar un marco de gobernanza de TI mediante políticas institucionales de seguridad, uso aceptable, gestión de contraseñas, control de software y dispositivos, asignación clara de roles y responsabilidades, así como capacitación continua del personal en buenas prácticas de seguridad informática.	2
APO03	0,89	Documentar y mantener actualizado el mapa de procesos institucionales, alineando los sistemas y activos tecnológicos a los procesos estratégicos y operativos, promoviendo la estandarización, automatización y mejora continua orientada a la atención ciudadana.	1

Tabla 7 – continuación

Proceso	Nivel inicial	Acción de mejora propuesta	Nivel esperado
APO12	0,44	Implementar una gestión activa de riesgos de TI mediante la identificación sistemática de riesgos, su registro en una matriz institucional, evaluación de impacto y probabilidad, definición de acciones de mitigación, asignación de responsables y capacitación básica del personal.	2
APO13	0,56	Establecer políticas básicas de seguridad de la información que regulen el uso de contraseñas, dispositivos, correo electrónico, almacenamiento seguro, controles de acceso y respaldos periódicos, fortaleciendo la protección de los datos institucionales.	4
DSS05	0,44	Definir e implementar procedimientos formales para la gestión de incidentes de seguridad, incluyendo mecanismos de reporte, respuesta, seguimiento y documentación, con el fin de garantizar la continuidad de los servicios tecnológicos.	3

3. Resultados

Los resultados se analizaron de manera progresiva conforme a las cinco fases metodológicas, en la Fase (i), se identificó la ausencia de políticas formales de seguridad y gobernanza. En la Fase (ii), la aplicación de encuestas y la herramienta PILAR evidenció salvaguardas en niveles L0 y L1. La Fase (iii) permitió cuantificar una madurez promedio de 0,60 y brechas significativas frente al nivel objetivo. En la Fase (iv), los factores de diseño de COBIT 2019 orientaron la priorización de procesos críticos. Finalmente, en la Fase (v), se formuló un plan integral de mejoras, validado mediante Delphi, que permitió alcanzar niveles de madurez superiores a $4{,}5$ en todos los dominios evaluados.

Como síntesis cuantitativa de la evaluación inicial, el nivel de madurez promedio fue 0,60, mientras que el nivel objetivo determinado por los factores de diseño fue 2,4, resultando en una brecha promedio de 1,8. Ningún dominio alcanzó el nivel 1 (realizado) inicialmente y, de forma consistente, la herramienta PILAR reveló que múltiples salvaguardas se encontraban en niveles L0 o L1 (no implementadas o incipientes).

Adicionalmente, se aplicó la prueba t de Student para muestras pareadas con el fin de comparar los puntajes promedio por dominio correspondientes a la primera y segunda ronda del método Delphi. En la Tabla 8, se muestran los resultados con una diferencia estadísticamente significativa ($t = -8{,}04$; $p = 0{,}0013$), lo cual respalda que las mejoras introducidas tuvieron un impacto positivo validado por los expertos. Este hallazgo fortalece la validez empírica del modelo propuesto para incrementar la madurez institucional.

Tabla 8: Resultados de la prueba t para muestras pareadas entre rondas Delphi

Métrica	Valor
Media de diferencias (Δ)	-0,404
Desviación estándar de diferencias	0,095
Número de dominios evaluados (n)	5
Estadístico t calculado	-8,04
Valor p (significancia bilateral)	0,0013

4. Conclusiones

La aplicación del marco COBIT 2019, junto con los factores de diseño y la metodología Delphi, permitió evaluar de manera estructurada la madurez de la gobernanza de tecnologías de la información en el GADP-Tufiño. Los resultados evidenciaron un nivel de madurez promedio inicial de 0,60 sobre 5, lo que refleja una ejecución incipiente de los procesos de TI, ausencia de documentación formal y limitados mecanismos de control institucional. Asimismo, la brecha promedio de 1,8 puntos respecto al nivel objetivo confirma la existencia de deficiencias estructurales en la gobernanza de TI, especialmente en procesos relacionados con la seguridad de la información, la gestión de riesgos y la gestión de incidentes.

El plan de mejora propuesto, alineado con COBIT 2019, permitió establecer acciones orientadas a la formalización de políticas, asignación de responsabilidades, fortalecimiento de controles, gestión de riesgos y atención de incidentes de seguridad. La validación mediante el método Delphi evidenció un alto nivel de consenso entre los expertos, alcanzando un índice de aceptación del 92 % en la primera ronda y del 100 % en la segunda. Este resultado demuestra la pertinencia, coherencia y viabilidad de las acciones propuestas para fortalecer la gobernanza de TI en una institución pública rural con recursos tecnológicos y organizativos limitados.

La selección de procesos COBIT 2019 como APO01, APO03, APO12, APO13 y DSS05 permitió focalizar el diagnóstico en áreas críticas para la institución. Además, a partir de las recomendaciones obtenidas durante la validación experta, se consideró pertinente incorporar el proceso MEA01, relacionado con el monitoreo, evaluación y valoración del desempeño y la conformidad. Esta incorporación fortalece el enfoque de seguimiento continuo, auditoría interna y control institucional, aspectos necesarios para garantizar la sostenibilidad de las mejoras planteadas.

En comparación con estudios similares, como el caso de la Municipalidad de Carrillo, Costa Rica [5], los hallazgos coinciden en evidenciar niveles iniciales bajos de madurez de TI en instituciones públicas. Sin embargo, el presente estudio se diferencia por integrar COBIT 2019 con la metodología Delphi como mecanismo de validación estructurada, permitiendo no solo diagnosticar brechas, sino también validar acciones de mejora con respaldo experto y enfoque cuantificable.

Finalmente, se concluye que COBIT 2019 constituye un marco adaptable y replicable para fortalecer la gobernanza de TI en instituciones públicas pequeñas. Su combinación con la metodología Delphi aporta una estrategia metodológica sólida para evaluar, priorizar y validar mejoras orientadas a la seguridad de la información, la gestión de riesgos, la continuidad de servicios tecnológicos y el alineamiento estratégico institucional. Como trabajo futuro, se recomienda implementar el plan de mejoras propuesto, aplicar las políticas de seguridad sugeridas y realizar evaluaciones periódicas que permitan verificar el avance real de la madurez de TI en el GADP-Tufiño.

Referencias

[1] M. Abdullah, A. Mustofa, and F. Rahman, “Leveraging cobit 2019 to implement it governance in public institutions,” *International Journal of Computer Applications*, vol. 975, no. 8887, pp. 25–30, 2020, aplicación en el Ministerio de Educación y Cultura de Indonesia. [Online]. Available: https://www.ijcaonline.org/archives/volume975/number8887/ijca920833.pdf

[2] Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), “Suplemento nétextordmasculine 328 - registro oficial 2, viernes 9 de junio de 2023,” *Registro Oficial*, vol. 328, no. 2, Jun. 2023.

[3] S. N. de Planificación, “Plan de desarrollo para el nuevo ecuador 2024–2025,” 2023.

[4] J. Tipán, “Modelo de ciberseguridad basado en cobit 2019 y nist para la empresa pública cnt,” Tesis de Maestría, Escuela Politécnica Nacional, Quito, Ecuador, 2022.

[5] A. Cortés, “Evaluación de la implementación de cobit 2019 en la municipalidad de carrillo, costa rica,” Master’s thesis, Universidad de Costa Rica, 2020. [Online]. Available: https://repositorio.ucr.ac.cr/handle/10669/82069

[6] D. Pauta, “Gestión de gobierno de ti basado en cobit 2019 para el colegio de bachillerato a distancia calderón,” Tesis de Maestría, Universidad Técnica del Norte, Ibarra, Ecuador, 2022. [Online]. Available: https://dialnet.unirioja.es/descarga/articulo/8219399.pdf

[7] E. Lompoliu and G. W. Tangka, “Enhancing it governance at bps manado: A cobit 2019 framework implementation study,” *TeIKa*, vol. 14, no. 1, 2024.

[8] M. Abdullah, A. Mustofa, and F. Rahman, "Cobit 2019 for enhanced ict governance: A case study," *International Journal of Computer Applications*, vol. 975, p. 8887, 2020. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/he-07-2020-0047/full/html

[9] L. Jaime and J. Barata, "How can floss support cobit 2019? coverage analysis and a conceptual framework," *Procedia Computer Science*, vol. 219, pp. 680–687, 2023, open access under CC BY-NC-ND license. [Online]. Available: https://doi.org/10.1016/j.procs.2023.01.339

[10] J. Felicia, J. F. Andry, F. Adikara, D. Y. Bernanda, and K. Christianto, "Leveraging cobit 2019 to measure the accounting software implementation in high schools for better transparency," *Journal of Computer Science*, vol. 20, no. 2, pp. 218–228, 2024. [Online]. Available: https://doi.org/10.3844/jcssp.2024.218.228

[11] C. J. P. Aya and A. M. S. Iguarán, "Modelo de gobierno y gestión de ti para desplegar la política de gobierno digital en las entidades tipo gobernación," Master's thesis, Fundación Universidad del Norte, Barranquilla, Colombia, 2019, tesis de Maestría en Gobierno de Tecnología Informática.

[12] R. Dionisio, Armand y Utama, "Aplicación de cobit 2019 en instituciones públicas del sudeste asiático," pp. 45–58, 2019.

[13] J. C. T. Rodríguez, "Gobierno de tic y sus beneficios para organizaciones pequeñas," Universidad Piloto de Colombia, Tech. Rep., 2023, trabajo académico. [Online]. Available: mailto:jose-torregroza@upc.edu.co

[14] B. Y. Fitriyani and A. H. Muhammad, "Cobit 2019 for enhanced ict governance: A case study at a higher education institution," *Journal of Information Systems and Informatics*, vol. 7, no. 1, pp. 45–62, 2025, licensed under Creative Commons Attribution 4.0 International License. [Online]. Available: http://journal-isi.org/index.php/isi/article/view/972

[15] D. S. Ramadhani, B. Sugiantoro, and A. Nugroho, "Optimizing it governance in bts.id: A cobit 2019-based capability level assessment," *Procedia Computer Science*, vol. 197, pp. 334–341, 2022. [Online]. Available: https://doi.org/10.1016/j.procs.2021.12.152

[16] A. Rizky, Erman, Yuniar, and Nurfajriani, "Audit tata kelola ti menggunakan cobit 2019 domain dss02," *Jurnal Teknologi dan Sistem Informasi*, vol. 4, no. 2, pp. 45–55, 2023. [Online]. Available: https://ejournal.uin-malang.ac.id/index.php/jtsi/article/view/25975

[17] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. Rolling Meadows, IL: ISACA, 2018.

[18] F. Hasson, S. Keeney, and H. McKenna, "Research guidelines for the delphi survey technique," *Journal of Advanced Nursing*, vol. 32, no. 4, pp. 1008–1015, 2000.

[19] ISACA, *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. Rolling Meadows, IL: ISACA, 2019.

[20] C. C. Nacional, "Pilar: Herramienta de análisis de riesgos," https://www.ccn-cert.cni.es, 2020, disponible en: https://www.ccn-cert.cni.es/seguridad/pilar.html.

Financiación

No aplica.