UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

" EVALUACIÓN DE LA MADUREZ DE SEGURIDAD INFORMÁTICA Y PROPUESTA DE MEJORAS PARA UN GOBIERNO AUTÓNOMO DESCENTRALIZADO PARROQUIAL RURAL DE TUFIÑO: UNA APROXIMACIÓN BASADA EN COBIT 2019 "

Trabajo de titulación previo a la obtención del título en Ingeniera en Tecnologías de la Información

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR:

Jenny Paulina Iñiguez Zambrano

DIRECTOR:

Ing. Marco Remigio Pusdá Chulde, PhD.

Ibarra – Ecuador 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	2100417548		
APELLIDOS Y NOMBRES:	Iñiguez Zambrano Jenny Paulina		
DIRECCIÓN:	Ciudadela 4 de octubre		
EMAIL:	jpiniguezz@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0985233423

DATOS DE LA OBRA	
TÍTULO:	EVALUACIÓN DE LA MADUREZ DE SEGURIDAD INFORMÁTICA Y PROPUESTA DE MEJORAS PARA UN GOBIERNO AUTÓNOMO DESCENTRALIZADO PARROQUIAL RURAL DE TUFIÑO: UNA APROXIMACIÓN BASADA EN COBIT 2019
AUTOR (ES):	Iñiguez Zambrano Jenny Paulina
FECHA: DD/MM/AAAA	08/09/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniera en Tecnologías de la Información
ASESOR /DIRECTOR:	Ing. Daisy Imbaquingo, PhD/ Ing. Marco Pusdá, PhD.

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 08 días del mes de septiembre de 2025

EL AUTOR:

(Firma).....

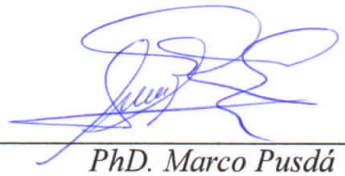
Nombre: Iñiguez Zambrano Jenny Paulina

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 04 de septiembre de 2025.

PhD. Marco Pusdá
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR
CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.



PhD. Marco Pusdá
C.C: 0401200951

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular " Evaluación de la madurez de seguridad informática y propuesta de mejoras para un Gobierno Autónomo Descentralizado Parroquial Rural de Tufiño: una aproximación basada en COBIT 2019 " elaborado por JENNY PAULINA IÑIGUEZ ZAMBRANO , previo a la obtención del título del Ingeniera en Tecnologías de la Información , aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

PhD. Marco Pusdá

C.C: 0401200951

Ing. Daisy Imbaquingo, PhD

C.C: 1002873048

DEDICATORIA

A Dios, por haberme dado la sabiduría, la fortaleza y la oportunidad de estudiar algo tan bonito e inspirador, sin su guía, este camino no habría sido posible.

A mis hijos Jefferson, Jeremy y Emily, porque son el motor de mi vida, la razón de cada esfuerzo y la inspiración más grande para seguir adelante, cada página de esta tesis lleva implícito su amor y su presencia en mi corazón.

A mi madre Carmen Zambrano, por ser ejemplo de lucha, entrega y amor incondicional, espero que este logro llene su corazón de orgullo, como ha llenado el mío de valores y fortaleza.

JENNY PAULINA IÑIGUEZ ZAMBRANO

AGRADECIMIENTO

Agradezco profundamente a todos los profesores que, a lo largo de esta etapa académica, compartieron sus conocimientos y me motivaron a superarme cada día. Cada clase, cada consejo y cada corrección fueron piezas fundamentales en este proceso.

Un especial agradecimiento al Msc. Marco Pusda, mi tutor de tesis, por su guía, paciencia y dedicación, su acompañamiento fue clave para alcanzar este logro.

Gracias a mi grupo de estudio Tesis por que SI, su ayuda constante marcaron la diferencia cuando más lo necesitaba, hicieron de este camino algo mucho más llevadero y divertido.

Y, sobre todo, gracias a mi amiga incondicional, compañera incansable de todas mis noches de estudio, esta meta también es tuya, sin ella nada de esto fuera posible.

JENNY PAULINA IÑIGUEZ ZAMBRANO

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Las entidades del sector público enfrentan grandes retos al momento de implementar una gobernanza efectiva de las Tecnologías de la Información (TI), en este contexto, la presente investigación se desarrolló en el GAD. Parroquial Rural de Tufiño, con el propósito de diseñar y validar un modelo metodológico basado en el marco COBIT 2019, orientado a medir y mejorar la madurez de los procesos de TI institucionales, la investigación adoptó un enfoque mixto y se estructuró en cinco fases: diagnóstico institucional, recolección de información, evaluación del nivel de madurez, aplicación de los factores de diseño del marco y validación de la propuesta, esta última se llevó a cabo mediante la metodología Delphi en dos rondas con la participación de diez expertos.Los resultados iniciales evidenciaron un nivel de madurez de 0,6, lo que reflejó una brecha considerable frente al nivel objetivo de 2,4. Posteriormente, la propuesta de mejora fue validada con niveles de aceptación del 92 % en la primera ronda y del 100 % en la segunda, en conclusión, la integración de COBIT 2019 con la metodología Delphi demostró ser efectiva para diagnosticar y fortalecer la gobernanza de TI en el GADP-Tufiño, mostrando además un alto potencial de aplicación en otras entidades del sector público o privado que busquen optimizar su gestión tecnológica.

Palabras clave: Gobernanza de TI, Seguridad Informática, COBIT 2019, PILAR

ABSTRACT

Public sector entities face significant challenges when implementing effective Information Technology (IT) governance. In this context, the present research was carried out at the Rural Parish GAD of Tufiño, with the objective of designing and validating a methodological model based on the COBIT 2019 framework, aimed at measuring and improving the maturity of institutional IT processes, the study followed a mixed-methods approach and was structured in five phases: institutional diagnosis, data collection, maturity level assessment, application of design factors from the framework, and validation of the proposed model. The validation was conducted through the Delphi methodology in two rounds with the participation of ten experts.The initial results revealed a maturity level of 0.6, indicating a significant gap compared to the target level of 2.4. Subsequently, the improvement proposal was validated with acceptance rates of 92 % in the first round and 100 % in the second, in conclusion, the integration of COBIT 2019 with the Delphi methodology proved to be effective in diagnosing and strengthening IT governance within the GADP-Tufiño, and it also demonstrated strong potential for replication in other public or private organizations seeking to optimize their technological management.

Keywords: IT Governance, Information Security, COBIT 2019, PILAR

CAPÍTULO I
INTRODUCCIÓN

1.1 Planteamiento del Problema

El Gobierno Autónomo Descentralizado Parroquial Rural de Tufiño enfrenta riesgos en la protección de su información y activos tecnológicos, la infraestructura de tecnologías de la información del GADP-Tufiño carece de una estructura adecuada y de políticas claras para gestionar sus activos tecnológicos, como servidores, sistemas de acceso y equipos de red.

Esta falta de organización y control provoca problemas de escalabilidad, integridad y disponibilidad, exponiendo la infraestructura a fallos y amenazas cibernéticas, además la ausencia de controles robustos de protección y monitoreo en los servidores deja vulnerables los datos institucionales, poniendo en riesgo la privacidad, exactitud y acceso a la información, ocasionando una situación grave tanto para la institución como para la ciudadanía.[1].

Además, la gestión deficiente de accesos y contraseñas dentro de la red agrava el riesgo, pues muchos usuarios, incluidos aquellos con acceso privilegiado,que no están obligados a usar contraseñas seguras ni a actualizarlas periódicamente, lo que facilita accesos no autorizados y aumenta el riesgo de robo de información [2].

Esta situación tiene graves repercusiones potenciales: la pérdida de información sensible podría afectar la capacidad del GADP-Tufiño para brindar servicios esenciales a la comunidad, socavando la confianza de la ciudadanía y generando riesgo en la estabilidad operativa de la institución.

La falta de medidas adecuadas de protección también puede conllevar responsabilidades legales y financieras, con la importancia de implementar marcos de gobernanza de TI como COBIT 2019 que mejoren la gestión de TI impactando la reputación del GADP-Tufiño Parroquial de Tufiño [3].

En el sector público, en el ámbito de la gobernabilidad es indispensable condiciones mínimas de seguridad y desarrollo, donde la protección informática es fundamental en la era digital, sin una estructura sólida para resguardar sus activos tecnológicos, el GADP- Tufiño al carecer de una adecuada infraestrcutura tecnológica pierde fuerza en su capacidad de ofrecer un entorno

confiable en los trámites en línea, siendo crucial para mantener relaciones institucionales y sociales efectivas, es fundamental establecer medidas de seguridad efectivas que promuevanr una cultura organizacional que priorice la mitigación de amenazas [4].

Desde una perspectiva de ingeniería, se llevó a cabo una auditoría técnica de la infraestructura de TI del GADP-Tufiño, incluyendo el monitoreo de servidores, redes y sistemas de seguridad actuales, para identificar vulnerabilidades específicas. Con base en este diagnóstico, se propuso una arquitectura de seguridad alineada con el marco COBIT 2019, que incluya la implementación de controles de acceso más estrictos y autenticación multifactorial, también se fortaleció la capacitación del personal en prácticas de ciberseguridad, asegurando así un entorno protegido y resiliente [4].

1.2 Objetivos

1.2.1 Objetivo General

Realizar una evaluación de la madurez de seguridad informática y propuesta de mejoras para un Gobierno Autónomo Descentralizado Parroquial Rural De Tufiño: una aproximación basada en COBIT 2019.

1.2.2 Objetivos Específicos

- Documentar los estándares de seguridad informática y la situación actual del GADP-Tufiño Descentralizado Rural de Tufiño en cuanto a la protección de la información y activos tecnológicos a través de una revisión bibliográfica que permita identificar fortalezas y debilidades en su infraestructura de TI.

- Desarrollar un plan de seguridad informática alineado con los estándares de COBIT 2019 con un enfoque específico en los dominios relacionados con la protección de la información y los activos es fundamental en este sentido resulta esencial garantizar la seguridad de los servidores prevenir accesos no autorizados y resguardar la infraestructura tecnológica de la institución.

- Evaluar el plan de seguridad desarrollado a través de expertos mediante el método de Delphi verificando el cumplimiento de los dominios del estándar COBIT 2019 para optimizar la resiliencia ante amenazas.

1.3 Alcance y delimitación

Se llevó a cabo la revisión bibliográfica de estándares de seguridad y buenas prácticas que permita identificar fortalezas y debilidades en la infraestructura de TI actual de la institución. Este diagnóstico brindó una base sólida para estructurar el plan de protección de la información y activos del GADP-Tufiño, incorporando prácticas clave de los procesos para Alinear, Planificar y Organizar (APO) relevantes.

Se desarrolló un plan de seguridad alineado con COBIT 2019, centrado en la protección de la información y activos del GADP-Tufiño, el plan incluyó medidas para asegurar los servidores, prevenir accesos no autorizados mediante autenticación y mejora la gestión de contraseñas [5].Este enfoque fue respaldado por las siguientes APO01 (Gestionar el Marco de Gestión de TI), APO03 (Gestionar la arquitectura empresarial), APO012 (Gestionar el Riesgo), APO13 (Gestionar la seguridad)

Garantizando la protección de la información y los activos informáticos, este enfoque integral asegura un entorno seguro y resiliente para la gestión tecnológica institucional, una vez desarrollado el plan, se ha evaluado mediante consultas a expertos utilizando el método Delphi, donde se obtuvo una retroalimentación especializada para optimizar el diseño propuesto, mejorando la resiliencia de la infraestructura ante posibles amenazas, garantizando que el plan no solo esté diseñado bajo estándares de calidad, sino que también responda adecuadamente a escenarios de riesgo reales.

1.4 Justificación

La presente investigación propone un plan de seguridad informática basado en el marco COBIT 2019, dirigido al GADP-Tufiño, su propósito es responder a la urgente necesidad de proteger la información y los activos digitales de las entidades públicas ante el creciente número de amenazas cibernéticas y las debilidades detectadas en la gestión de la seguridad, el plan está orientado a asegurar que la información se preserve con integridad, disponibilidad y confidencialidad, en concordancia con lo establecido en la normativa aplicable. [6].

En el marco del Plan de Desarrollo para el Nuevo Ecuador 2024-2025, dentro de las directrices establecidas en la política 3.12, se busca fortalecer la ciberseguridad en el ámbito de las telecomunicaciones, para alcanzar este objetivo, se han definido diversas estrategias, entre las cuales se destacan:

a) Manejar de forma óptima los incidentes y vulnerabilidades en ciberseguridad que puedan comprometer los servicios de telecomunicaciones, asegurando la seguridad de la infraestructura digital y la confianza de los usuarios.

b) Diseñar e impartir programas de formación y concienciación sobre ciberseguridad, dirigidos a la ciudadanía, empresas y servidores públicos, con el propósito de mejorar sus habilidades tecnológicas y promover una cultura de protección en el ámbito virtual [7].

Por esta razón, el presente proyecto proporciona un marco definido y adecuado para la gestión integral de la seguridad de la información en el GADP-Tufiño, utilizando los estándares de COBIT 2019. Donde se desarrolló el plan de seguridad que no solo atendió las necesidades específicas de esta institución, sino que también podrá ser un ejemplo a seguir para otras organizaciones en el ámbito público, que mejorará tanto la gobernanza como la gestión de riesgos [8].

El principal beneficiario de esta propuesta es el GADP-Tufiño, al lograr la sistematización de la seguridad en sus sistemas de información y en sus procesos internos, por lo cual de esta forma indirecta, también se benefició la comunidad de Tufiño, al fortalecerse la protección de datos y ofrecerse un servicio público más eficiente, lo que incrementó la confianza de los ciudadanos en su gobierno local, a través de sta iniciativa se contribuye a establecer un entorno seguro para la gestión de la información, garantizando la confidencialidad de los datos y reduciendo el riesgo de accesos no autorizados o ciberataques.

Además, la implementación de mejoras continuas en la gestión pública promueve la transparencia y facilita la rendición de cuentas, en cumplimiento con las normativas vigentes laa ausencia de un marco de seguridad claramente definido en el GADP-Tufiño ha evidenciado debilidades en la gestión de la información. La adopción del estándar COBIT 2019 ha permitido identificar y gestionar de manera más eficiente los riesgos asociados a la seguridad informática. [9].

Abordando la ausencia de un marco de seguridad claro en el GADP-Tufiño, que ha resultado en vulnerabilidades en la gestión de la información, el desarrollo del estándar COBIT 2019 permitió identificar y manejar eficazmente los riesgos relacionados con la seguridad informática, solucionando problemas específicos que han surgido por la falta de control y protección de datos [10], desde un punto de vista técnico, la investigación integró herramientas y metodologías avanzadas para gestionar riesgos y la seguridad en TI, lo que enriqueció el campo de la ingeniería informática a través de este caso de estudio que se lo pudo aplicar en el sector público.

Interpretar y ajustar marcos de control como COBIT 2019 a entornos particulares, lo que impulsó la investigación y la creación de estrategias más efectivas para la protección de la información y los activos digitales [1], además, esta investigación permitió adquirir conocimientos prácticos sobre la aplicación del marco COBIT 2019 y la gestión de la seguridad de la información en el contexto de la gobernanza, el aprendizaje obtenido resultó valiosos tanto para estudiantes como para profesionales interesados en implementar marcos de seguridad en organizaciones del sector público, dentro de un entorno real y aplicado.

El proceso de aprendizaje permitió aplicar de mejor manera la protección de la información y garantizar la continuidad en la prestación de servicios a la comunidad, incrementando la confianza en la gestión pública en el GAD- Tufiño, promoviendo el aprendizaje y la capacitación continua en todos los ámbitos de seguridad informática dentro del sector público, donde se utilizó un enfoque práctico y metodológico.

Además, se reforzó el estudio de la seguridad en TI dentro de marcos de control como COBIT 2019, incentivando futuras investigaciones en otros contextos públicos [5], evitando pérdidas financieras derivadas de incidentes de seguridad, optimizando el uso de recursos mediante la prevención de riesgos en la seguridad informática, con un mejor manejo de datos y la generando confianza en el GADP-Tufiño, factores clave para la reputación y la responsabilidad social de cualquier institución pública, siendo un recurso de aprendizaje y guía para implementar marcos de seguridad informática en las instituciones tanto educativas como administrativas de la región.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

En 2018, ISACA lanzó COBIT 2019, una actualización que ofreció mayor flexibilidad y personalización a las organizaciones. El marco se orienta a la gobernanza y gestión de las tecnologías de la información (TI), permitiendo a las organizaciones alinear sus estrategias tecnológicas con los objetivos empresariales [11], COBIT 2019 ha desempeñado un papel esencial en la creación de planes de seguridad informática dentro del sector público, proporcionando un enfoque personalizado para las necesidades particulares de cada institución y facilitando la identificación y manejo de riesgos [12].

En 2017, el gobierno ecuatoriano implementó la Política Nacional de Ciberseguridad, cuyo propósito es fortalecer la protección cibernética en las entidades estatales [13]. Esta normativa establece directrices para proteger los datos y los activos tecnológicos, fomentando la implementación de buenas prácticas y el uso de marcos como COBIT 2019 para fortalecer la ciberseguridad en las entidades gubernamentales, como consecuencia de estas iniciativas, el GADP-Tufiño ha identificado a las Tecnologías de la Información y la Comunicación (TIC) como un recurso fundamental e indispensable de implementar en la institución y así se obtuvo el mejoramiento de la gestión institucional.

No obstante, actualmente carece de un plan sólido de seguridad TI y asigna recursos limitados a productos y servicios tecnológico lo que expone su sistema a vulnerabilidades [14], esto resalta la importancia de adoptar estrategias que garanticen la continuidad de las operaciones, refuercen la infraestructura tecnológica y respondan a los requerimientos internos, al mismo tiempo que optimizan la calidad de los servicios brindados a la comunidad.

2.1.1 Situación Organizacional

El GADP-Tufiño cuenta con una infraestructura tecnológica y organizativa que respalda su operatividad, atención ciudadana y gestión de proyectos comunitarios, sus activos están distribuidos entre las áreas administrativa, operativa y de tecnología, complementados por un sitio web institucional.

En el Área Administrativa, los principales recursos incluyen un servidor centralizado que gestiona los servicios tecnológicos, un sistema contable para la administración financiera, un rack con 12 puntos de red para la distribución de conectividad, una computadora de escritorio y 10 Thin Clients utilizados para tareas operativas básicas, esta área se enfoca en la gestión contable, la administración de recursos y el soporte interno, asegurando la eficiencia en los procesos administrativos y financieros.

El Área Operativa cuenta con una computadora de escritorio y 4 computadoras portátiles que se utilizan para la atención al público, elaboración y ejecución de proyectos comunitarios y algunas actividades en campo, este equipamiento facilitó el monitoreo, planificación y el contacto directo con los ciudadanos, contribuyendo así al cumplimiento de los objetivos del GADP-Tufiño, el sitio web Institucional desempeña un papel clave en la difusión de información y servicios en línea, favoreciendo la claridad y el flujo de información con la comunidad.

Aunque es administrada de manera indirecta por el personal del GADP-Tufiño, ya que está concebida como una herramienta fácil de usar que fomenta una conexión sólida entre la institución y la comunidad, la Conexión Tecnológica constituye un pilar fundamental, con un servidor conectado al rack de red que distribuye la conectividad a todos los equipos del GADP-Tufiño, incluyendo los Thin Clients, la computadora de escritorio y las portátiles.

El sistema contable funciona desde el servidor y solo puede usarse en dispositivos autorizados, asegurando el entorno y la eficiente en la gestión de la información, los activos tecnológicos y organizativos permitieron al GADP-Tufiño mostrar un servicio integral y confiable a la ciudadanía, aplicando la gestión pública y avances en la ejecución de proyectos que beneficien a los usuarios de manera directa.

Debido a la importancia de los recursos tecnológicos en la administración institucional, se vuelve esencial aplicar el estándar COBIT 2019 para evaluar los riesgos en materia de TI, el uso de este marco de control facilita la identificación, evaluación y mitigación de los riesgos vinculados a la infraestructura tecnológica, garantizando la continuidad operativa como la protección de los datos sensibles de la institución y de la ciudadanía, al implementar COBIT 2019 hubo diversos beneficios, entre los cuales se destacan los siguientes:

- Gestión Integral del Riesgo: Identifica vulnerabilidades y amenazas en sistemas críticos, como el servidor, la red y el sistema contable.

- Optimización de Recursos Tecnológicos: Garantizando una gestión pública de la infraestructura tecnológica, donde se reduce las interrupciones y mejora el desempeño.

- Fortalecimiento de la Gobernanza de TI: Establece procesos claros de control y auditoría, alineando las decisiones tecnológicas con los objetivos estratégicos.

- Mejora de la Confianza Ciudadana: Al garantizar la seguridad y disponibilidad de los servicios tecnológicos, se incrementa la percepción de confianza en la gestión pública [15].

En conjunto, la incorporación de COBIT 2019 contribuyo a crear un entorno tecnológico más seguro y eficiente, respaldando los objetivos institucionales y fortaleciendo el servicio a la comunidad, la relación entre COBIT 2019 y la gobernanza, destacan cómo la integración de estos marcos puede mejorar la resiliencia organizacional y la alineación entre los procesos de TI y los objetivos de continuidad de las organizaciones.

Los beneficios de utilizar COBIT 2019 en la BCM, como la mejora en la identificación de riesgos, la alineación estratégica, la cultura de mejora continua y la capacitación del personal, siendo esto relevante en la capacidad de respuesta ante crisis y garantizar la continuidad operativa en el sector público [16], la importancia del estándar COBIT 2019 reside en su habilidad para proporcionar un enfoque completo y estructurado, que permite tomar decisiones fundamentadas, incrementar la eficacia operativa y aprovechar de manera óptima los recursos públicos.

Asimismo, al estructurar un modelo de gestión para las Tecnologías de la Información y Comunicación (TIC), se proporciona una guía que orienta la ejecución de acciones a corto, mediano y largo plazo, garantizando la eficacia y sostenibilidad de los procesos tecnológicos dentro del GADP-Tufiño, la combinación estratégica de las TIC con los objetivos institucionales se convierte en un componente fundamental para la gobernanza tecnológica, conforme a lo establecido por el marco COBIT 2019. [13].

Se destaca la importancia de invertir en tecnología y que estas estén alineadas de manera estrecha con la estrategia y los objetivos institucionales, como condición fundamental para maximizar su retorno, al existir ausencia de esta articulación estratégica puede conducir a un uso ineficiente de los recursos tecnológicos, lo que a su vez limita la capacidad de la organización para cumplir sus metas y responder con agilidad a los cambios del entorno organizacional.

Por lo tanto, la implementación de un gobierno TIC efectivo debe centrarse en garantizar que las decisiones tecnológicas apoyen y potencien la dirección estratégica de la organización [14].

2.2 Estandares de Seguridad

Los estándares de calidad son directrices y criterios que cada organización o empresa utilizan para generar un entorno seguro de sus productos y servicios y que por medio de esto cumplan con las expectativas y requisitos del cliente, en los últimos tiempos, estos estándares han experimentado una evolución, ajustándose a las demandas cambiantes de los mercados y las tecnologías. Los tipos y ventajas de los estándares de calidad se han aplicado de manera más común, lo que ha llevado a las organizaciones a adoptar estos estándares de seguridad para enfrentar los desafíos que surgen [17].

La norma ISO/IEC 27001 es reconocida a nivel internacional como un estándar clave para la gestión de la seguridad de la información, este marco proporciona lineamientos esenciales para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI), a continuación, se describen algunos de los aspectos más relevantes que abarca como referencia fundamental en el ámbito de la seguridad:

Evaluación de Riesgos:Este estándar destaca la relevancia de llevar a cabo evaluaciones de riesgos como un proceso fundamental para identificar y analizar las amenazas que afectan la seguridad de la información, permitiendo a cada organización establecer prioridades y definir acciones específicas orientadas al fortalecimiento de su sistema de seguridad. [15].

Controles de Seguridad: Contiene un conjunto de medidas de seguridad que pueden ser implementadas para salvaguardar la información del GADP-Tufiño, agrupando estas medidas en algunas categorías, como son controles físicos, técnicos y organizativos.

Cumplimiento Legal y Normativo:Asimismo, la norma resalta la importancia de asegurar el cumplimiento de las normativas y disposiciones legales relacionadas con la seguridad de la información, lo que permite evitar posibles sanciones, sino que también contribuye a proteger la imagen y credibilidad de la organización frente a sus partes interesadas.

Mejora Continua: Uno de los principios fundamentales de la norma ISO/IEC 27001 es la promoción de la mejora continua dentro de las organizaciones, permitiendo evaluar y optimizar de manera constante el Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de responder eficazmente a la evolución de las amenazas y a los cambios estructurales que puedan surgir dentro de la propia organización [18].

Concienciación y Formación: La norma enfatiza la importancia de concienciar y entrenar al personal en seguridad de la información, asegurando que cada miembro comprenda su rol en la protección de los datos.

Documentación y Registro: La ISO/IEC 27001 establece que las organizaciones deben conservar documentación apropiada y criterios vinculados a su SGSI, lo que facilita la auditoría y evaluación del sistema [19].

La ISO/IEC 27001 sigue un enfoque estructurado y metódico que facilita la administración de la seguridad informática, con el fin de ayudar a las organizaciones a proteger sus activos de información, lo que, a su vez, refuerza la confianza de sus partes interesadas [20].

La norma ISO/IEC 27002 ofrece directrices sobre las mejores prácticas en la implementación de controles de seguridad de la información, actuando como un complemento a la ISO/IEC 27001, la cual define los requisitos necesarios para establecer un Sistema de Gestión de Seguridad de la Información (SGSI).

La ISO/IEC 27002 brinda orientación a las organizaciones en la selección, aplicación y administración de los controles de seguridad, con la finalidad de proteger de manera eficaz los activos informáticos y gestionar riesgos asociados en el entorno digital.

[21].

2.2.1 Controles de Seguridad

La norma esta compuesta por un conjunto de medidas de seguridad que se pueden implementarse en protección de la información, estas acciones se organizan en diversas categorías, incluyendo:

- Controles físicos y ambientales: Incluye la protección de las instalaciones y los equipos.
- Controles técnicos: Está enfocado en resguardar la infraestructura tecnológica, mediante el control de accesos y el uso de criptografía.

2.2.2 Estructura de los Controles

ISO/IEC 27002 proporciona una lista de controles que se pueden adaptar a las necesidades específicas de cada organización. Cada control incluye:

- Descripción: Una explicación del control y su propósito.
- Objetivos: Los objetivos que se buscan alcanzar con la implementación del control.

- Implementación: Directrices sobre cómo implementar el control de manera efectiva.

2.2.3 Mejora Continua

La norma subraya la relevancia de la mejora continua dentro de cada organización, especialmente en la gestión de la seguridad de la información. Las organizaciones deben evaluar y actualizar de manera constante sus controles para ajustarse a los cambios en el entorno de amenazas y en la estructura organizativa [22].

a) Integración con ISO/IEC 27001:

ISO/IEC 27002 es particularmente valiosa para las organizaciones que desean cumplir con los requisitos de ISO/IEC 27001, ya que ofrece una estructura práctica para implementar los controles esenciales para un SGSI eficiente.

a) Beneficios:

- Disminuir los riesgos asociados a la protección de la información.
- Cumplir con requisitos legales y reglamentarios.
- Fortalecer la confianza de los grupos de interés en la administración de la seguridad de la información.

gestión de la seguridad de la información. La ISO/IEC 27002 es una norma clave para la gestión de la seguridad de la información, ya que proporciona directrices prácticas y un marco de referencia para implementar controles de seguridad efectivos en las organizaciones.

2.3 COBIT 2019

COBIT 2019 constituye un marco integral diseñado para fortalecer el gobierno y la gestión de la información y la tecnología en las organizaciones, dentro de un contexto digital dinámico y en permanente evolución, se vuelve imprescindible adoptar un enfoque estructurado que asegure la alineación entre las capacidades tecnológicas y los objetivos estratégicos de la entidad [23], en un entorno donde el avance tecnológico es acelerado y la tecnología se ha consolidado como un factor clave para el éxito organizacional, la gestión de la información y de las Tecnologías de la Información (TI) ha pasado a ser una prioridad estratégica de gran relevancia.

COBIT 2019 se desarrolló como una solución eficaz, que proporciona un marco sólido permitiendo a las organizaciones gestionar y optimizar sus recursos tecnológicos existentes de una forma eficiente, este enfoque no solo pretende integrar la TI con los objetivos estratégicos de la empresa, sino que también fomenta la creación de valor y la mitigación de los riesgos que están vinculados al uso de la tecnología [24].

Las versiones anteriores de COBIT, específicamente COBIT 4.1 y COBIT 5, Establecieron los cimientos para la creación de un marco de gobernanza y administración de TI más sólido y ajustado a las demandas actuales de las organizaciones [25].

COBIT 4.1, fue Lanzada en 2007, esta versión introduce un enfoque que está organizado de manera que la administración de la tecnología de la información, tenga la importancia y alineación de objetivos tecnológicos con las metas corporativas, además, proporciona una herramientas y procesos destinados a la implementación tanto de controles como de evaluación del rendimiento de cada uno de los recursos tecnológicos [26].

En 2012, COBIT 5 marcó un avance significativo al unificar principios de gobernanza y gestión en un único conjunto de directrices, esta versión puso el foco en maximizar el valor derivado de las inversiones en TI, promoviendo una visión integral que no solo abarcaba la gestión de riesgos, sino también la alineación con otros estándares y marcos internacionales.

Además, presentó el concepto de çatalizadores", factores fundamentales que influyen directamente en la efectividad del gobierno y la administración de la TI [27], COBIT 2019 supone un paso adelante al expandir los principios establecidos en versiones anteriores.

Mediante la incorporación de ideas innovadoras, como en las áreas de enfoque y los elementos de diseño, que facilitan ajustar el marco a las características y requerimientos específicos, COBIT 2019 fortalece la correlación con estándares internacionales y mejores prácticas, que facilitan su implementación en ambiente empresarial en constante cambio.

Al incorporar aprendizajes de COBIT 4.1 y COBIT 5, Esta versión se presenta como una herramienta más precisa y adaptable, creada para abordar los desafíos actuales de la gobernanza de TI y maximizar el valor que las organizaciones pueden obtener de sus inversiones tecnológicas [28].A diferencia de sus predecesores, COBIT 2019 introduce conceptos innovadores que permiten una mayor flexibilidad y adaptabilidad, como se muestra en la Fig. **??**, lo que facilita su implementación en diversos contextos organizacionales.

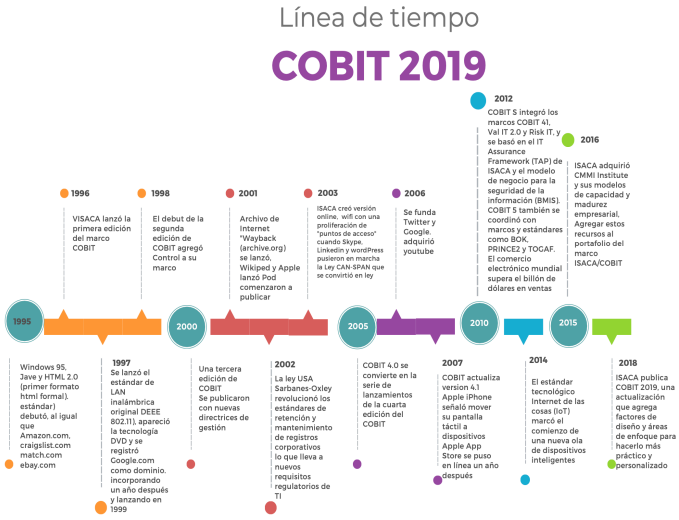


Fig. 1.. Línea de tiempo. [29]

Con un enfoque en la mejora constante y la incorporación de las mejores prácticas internacionales, este marco se transforma en una herramienta esencial para los líderes empresariales que desean reforzar su capacidad de adaptarse a un entorno en evolución.

A lo largo de este análisis, se examinarán los componentes principales de COBIT 2019, su estructura y cómo puede ser empleado para mejorar la efectividad y eficiencia en la gestión de la gobernanza de TI [30]. Este marco ofrece no solo directrices y buenas prácticas, sino también la flexibilidad necesaria para ajustarse a las necesidades particulares de cada organización, adaptándose a sus características y desafíos específicos [31].

COBIT 2019, Mediante sus componentes, su objetivo es respaldar la toma de decisiones estratégicas, optimizar el uso de los recursos tecnológicos y garantizar que las inversiones en tecnología generen valor, en este sentido, resulta crucial analizar los principios y objetivos que lo fundamentan, así como su importancia en el contexto actual de la gobernanza de TI [32].

Implica la implementación de prácticas y estrategias diseñadas para reforzar la gobernanza de la tecnología de la información (TI) y los recursos de información en una organización, este enfoque es fundamental para asegurar un uso eficiente y efectivo de los recursos tecnológicos, alineándolos con los objetivos empresariales y fomentando la creación de valor [33], se espera que los resultados de esta investigación proporcionen una visión profunda sobre el estado de la gestión de TI en los GADP-Tufiño municipales, junto con sugerencias prácticas para implementar un modelo de gobernanza de TI basado en COBIT 2019.

Esto no solo reforzará la gestión de los recursos tecnológicos, sino que también permitirá a los municipios alinearse de manera más eficiente con sus objetivos estratégicos [34]. En un

entorno donde la tecnología avanza rápidamente y es fundamental para el éxito empresarial, la gobernanza de la información y la tecnología (TI) se ha convertido en un aspecto esencial.

COBIT 2019 surge en respuesta a la necesidad de seguridad tecnológica y ofrece un marco robusto que ayuda a las organizaciones en la gestión y optimización eficiente de sus recursos tecnológicos [16], este marco no solo tiene como objetivo alinear la TI con los objetivos estratégicos de la organización, sino que también promueve la creación de valor y la disminución de los riesgos asociados al uso de la tecnología.

A diferencia de sus predecesores, COBIT 2019 introduce conceptos innovadores que permiten una mayor flexibilidad y adaptabilidad, lo que facilita su implementación en diversos contextos organizacionales [35].

Con un enfoque en la mejora constante y la adopción de las mejores prácticas internacionales, este marco se convierte en una herramienta clave para los líderes empresariales que buscan fortalecer su habilidad para adaptarse a un entorno en continua evolución [36].A lo largo de este análisis, se examinarán los componentes fundamentales de COBIT 2019, su estructura y cómo puede ser aplicado para mejorar la efectividad y eficiencia en la gobernanza de TI [37].

En un entorno digital en constante evolución, donde la tecnología es la clave para la eficiencia de las organizaciones, una gestión adecuada de los recursos tecnológicos resulta esencial, COBIT 2019 proporciona un marco completo que no solo proporciona directrices para la gobernanza y gestión de TI, sino que también asegura que las tecnologías estén alineadas con los objetivos estratégicos de las organizaciones [38].

Para el GADP-Tufiño, implementar de COBIT 2019 representó una herramienta primordial que mejoró la gobernanza tecnológica, optimizó los recursos y aseguró la protección de los activos digitales fundamentalmente, este marco promueve una gestión eficiente en el manejo riesgos tecnológicos, que impulsa la creación de valor mediante la disminución de amenazas y la mejora constante de los procesos operativos [1].

En este contexto, se emplearán los siguientes subdominios de COBIT 2019 para satisfacer las necesidades particulares del GADP-Tufiño:

APO01 - Gestionar el marco de gobierno: Proporciona las bases para estructurar la gobernanza de TI, asegurando la alineación con los objetivos estratégicos del GADP-Tufiño.

APO03 - Gestionar la arquitectura empresarial: Garantiza que la infraestructura tecnológica esté diseñada para satisfacer las demandas operativas y estratégicas de la organización.

APO12 - Gestionar los riesgos de TI: Ayuda a identificar, analizar y mitigar los riesgos tecnológicos que pueden afectar la operación y los servicios críticos del GADP-Tufiño.

APO13 - Gestionar la seguridad: Asegura la protección de los datos y activos digitales mediante controles que garantizan la confidencialidad, integridad y disponibilidad de la información.

DSS05 - Gestionar la seguridad de los servicios: Define controles específicos para prevenir y reaccionar ante incidentes de seguridad, reforzando la continuidad de los servicios tecnológicos.

La aplicación de estos subdominios permitirá no solo una gestión más eficaz de los recursos tecnológicos, sino también una mayor confianza en la seguridad y eficiencia de las operaciones del GADP-Tufiño, promoviendo el cumplimiento de los objetivos estratégicos y administrativos.

2.3.1 El subdominio APO01 Gestionar el Marco de la Gestión TI

Este subdominio se enfoca en la alineación, planificación y organización en la administración de las tecnologías de la información (TI), su objetivo es garantizar que la TI apoye los objetivos estratégicos de la organización y se gestione de forma eficiente para maximizar su contribución de valor.

- Alineación Estratégica: APO01 Tiene como objetivo garantizar que las iniciativas de TI estén en sintonía con la misión, visión y objetivos estratégicos de la organización. Esto incluye comprender las necesidades de las partes interesadas y cómo la TI puede abordarlas.

- Planificación de TI: Se centra en desarrollar una estrategia de TI que respalde los objetivos de la organización, la Fig. 2 abarca la planificación de recursos, la gestión de riesgos y la identificación de oportunidades para la innovación [34].

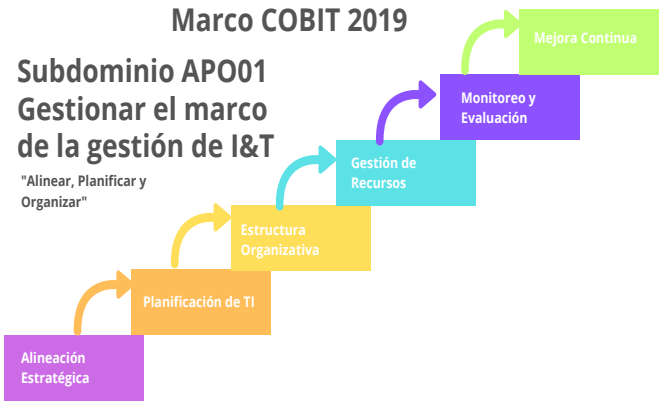


Fig. 2. APO01 [29]

- Estructura Organizacional: APO01 fomenta el establecimiento de una estructura organizativa que favorezca la gobernanza de TI, abarcando la definición de roles y responsabilidades específicas.
- Gestión de Recursos: Se enfoca en la administración eficiente de los recursos de TI, garantizando que se empleen de manera efectiva para alcanzar los objetivos planteados.
- Supervisión y Evaluación: Implica la puesta en marcha de mecanismos para supervisar el rendimiento de TI y evaluar si se están logrando los objetivos establecidos.
- Optimización Continua: Promueve una cultura de mejora constante en la gestión de TI, donde se revisen y ajusten de manera periódica las estrategias y procesos según los resultados obtenidos.

2.3.2 El subdominio APO03 Gestionar la Arquitectura Empresarial

- Sistemas de Comunicación: Abarcan todos los medios de comunicación que facilitan el intercambio de datos entre diversos dispositivos y sistemas dentro de la organización. Esto puede incluir redes locales (LAN), redes de área amplia (WAN) y conexiones a Internet.

  La Fig. 3 muestra cómo se desarrolla el APO03.

Fig. 3. APO03 [29]

- Equipos de Red: Dispositivos como routers, switches, firewalls y puntos de acceso que facilitan la conectividad y la seguridad de la red.

  Conexiones entre Componentes

- Interconexión de Sistemas: Las aplicaciones, bases de datos y otros sistemas deben estar conectados para permitir el flujo de información. Esto incluye conexiones entre sistemas

internos y externos, así como entre diferentes aplicaciones que pueden necesitar compartir datos.

- Conexión de Servicios: Las redes posibilitan la integración de diversos servicios y aplicaciones, promoviendo la comunicación y cooperación entre departamentos y equipos [38]. Seguridad de la Red

- Protección de Datos: La arquitectura debe incluir medidas de seguridad para proteger la información que se transmite a través de la red. Esto puede incluir firewalls, sistemas de detección de intrusos y cifrado de datos.

- Políticas de Acceso: Definir quién tiene acceso a qué recursos dentro de la red es crucial para mantener la seguridad y la integridad de la información.

- Facilitación de Nuevas Tecnologías: Una infraestructura de red adecuada es clave para la implementación de nuevas tecnologías, como la computación en la nube, el Internet de las Cosas (IoT) y las soluciones de big data.

- Escalabilidad: La red debe ser capaz de escalar para soportar el crecimiento de la organización y la incorporación de nuevas tecnologías y servicios.

- Diagramas de Red: Se utilizan diagramas para representar visualmente la arquitectura de red, mostrando cómo se conectan los diferentes componentes y sistemas.

- Documentación: Mantener una documentación clara de la arquitectura de red es esencial para la gestión del conocimiento y la planificación de cambios fundamentales que forman parte de la infraestructura tecnológica de una organización.

2.3.3 El subdominio APO12 Gestionar el Riesgo

El proceso APO12, Gestión de Riesgos, es una parte clave dentro del marco de gobernanza y administración de TI, especialmente alineado con las pautas de COBIT 2019. Este proceso se enfoca en identificar, evaluar y gestionar los riesgos relacionados con la tecnología de la información (TI), garantizando que estos riesgos sean tratados de manera que respalden los objetivos estratégicos de la organización.

La Fig. 4 muestra el proceso APO12, Gestión de Riesgos, que constituye un elemento esencial dentro del marco de gobernanza y gestión de TI, alineado de manera específica con las directrices de COBIT 2019. Su objetivo principal es identificar, evaluar y gestionar los riesgos

asociados a la tecnología de la información (TI), asegurando que estos sean manejados de forma que contribuyan al cumplimiento de los objetivos estratégicos de la organización [34].

Fig. 4. APO12 [29]

Funciones Clave del APO12

- Identificación de Riesgos: Este proceso consiste en reunir información pertinente acerca de los riesgos potenciales que podrían impactar a la organización, abarcando riesgos tecnológicos, operativos, de seguridad y de cumplimiento con las normativas.
- Análisis de Riesgos: Una vez identificados, los riesgos se analizan para determinar su probabilidad de ocurrencia y su impacto potencial en la organización. Este análisis ayuda a priorizar los riesgos y a decidir cuáles requieren atención inmediata [19].
- Análisis de riesgos: Se determina el nivel de riesgo que la organización está dispuesta a aceptar, lo que implica definir criterios para identificar qué riesgos son inaceptables y cuáles pueden ser asumidos.
- Creación de estrategias de reducción de riesgos: Se elaboran y ponen en práctica estrategias para disminuir los riesgos identificados, lo que puede incluir la implementación de controles técnicos, políticas de seguridad, formación del personal y planes de acción ante incidentes.
- Monitoreo y evaluación: El proceso no termina con la aplicación de las estrategias de mitigación de riesgos. Es crucial realizar un seguimiento continuo de los riesgos y valorar la efectividad de las medidas implementadas. Esto incluye revisar periódicamente el registro de riesgos y ajustar las estrategias cuando sea necesario [1].

En el campo de la seguridad de la información, el propósito fundamental es proteger los datos frente a pérdidas, accesos no autorizados o alteraciones indebidas, priorizando la garantía de la confidencialidad, integridad y disponibilidad de la información, también es esencial considerar otros principios igualmente relevantes, como la autenticidad, entre otros factores que contribuyen a un entorno seguro y confiable. [24].

La razón fundamental para implementar medidas de protección relacionadas con la seguridad de la información radica en el interés propio de las instituciones o personas responsables de los datos. Esto se debe a que cualquier pérdida o modificación de la información puede ocasionarles daños, ya sean materiales o intangibles [36].

2.3.4 El subdominio APO13 Gestionar la Seguridad

La APO13, dentro del marco de trabajo COBIT 2019, se encarga de definir, operar y monitorear un Sistema de Gestión de Seguridad de la Información (SGSI).

- Definición del SGSI: Establecer un marco claro que incluya políticas, procedimientos y controles necesarios para proteger la información de la organización [35].
- Operación del SGSI: Implementar y gestionar las actividades diarias relacionadas con la seguridad de la información, asegurando que se cumplan las políticas y procedimientos establecidos.
- Monitoreo del SGSI: Realizar una evaluación continua de la efectividad del SGSI mediante el monitoreo de los controles de seguridad, la identificación de incidentes y la realización de auditorías [37].
- En la Fig. 5 de Mejora continua, se identifican los resultados del monitoreo para realizar ajustes y mejoras en el SGSI, adaptándose a nuevos riesgos y cambios en el entorno organizacional [39].

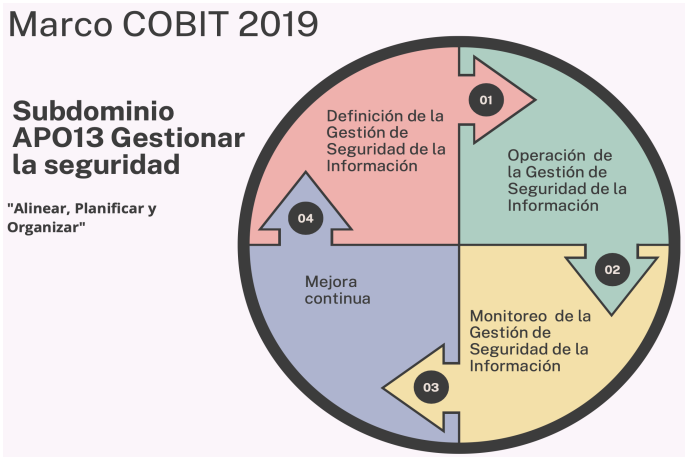


Fig. 5. APO13 [29]

El APO12 y APO013 no opera de manera aislada; está interconectado con otros procesos dentro del marco de COBIT, por ejemplo.

La gestión de riesgos debe estar alineada con la gestión de servicios (DSS) y la gestión de recursos (APO), asegurando que las decisiones sobre TI se tomen con una comprensión clara de los riesgos involucrados, los procesos del dominio DSS están orientados a ofrecer servicios de TI confiables, eficientes y efectivos, garantizando una gestión adecuada de las operaciones tecnológicas, que abarca el soporte técnico, la resolución de problemas, la seguridad y la continuidad [33].

DSS Deliver, Service, and Support (Entregar, Servir y Soportar).

Este dominio se enfoca en la operación y el soporte de los servicios de TI, asegurando que los procesos y actividades tecnológicas estén alineados con los objetivos de la organización.

2.3.5 Dominio DSS05 Gestión de la seguridad de los servicios

Dentro del marco COBIT 2019, el proceso DSS05 hace referencia a la Gestión de los Servicios de Seguridad de TI (Manage Security Services), su enfoque principal es asegurar la protección efectiva de los servicios tecnológicos, mediante la aplicación de controles y mecanismos que salvaguarden la confidencialidad, integridad y disponibilidad de la información, este proceso tiene como objetivo implementar prácticas adecuadas que protejan tanto los datos como los activos tecnológicos de la organización, como se puede ver en la Fig. 6, para abordar los riesgos relacionados con la seguridad de la información [19].

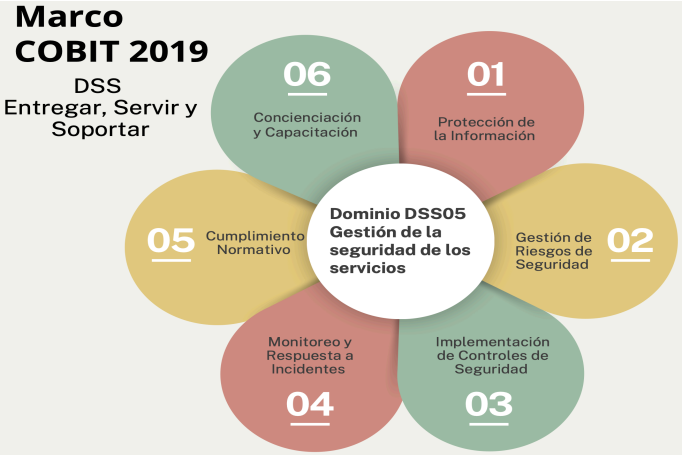


Fig. 6. APO13 [29]

- Protección de la Información: Asegura que la información y los activos de TI estén protegidos contra accesos no autorizados, alteraciones y destrucción.
- Gestión de Riesgos de Seguridad: Implica la identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información y los servicios de TI.
- Implementación de Controles de Seguridad: Establece y mantiene controles de seguridad adecuados, como firewalls, sistemas de detección de intrusos (IDS), y políticas de acceso, para proteger los servicios de TI.
- Monitoreo y Respuesta a Incidentes: Asegura que haya procesos en marcha para monitorear la seguridad de los servicios de TI y responder de manera efectiva a incidentes de seguridad.
- Cumplimiento Normativo: Garantiza que la organización cumpla con las regulaciones y estándares de seguridad aplicables, como ISO 27001, para la gestión de la seguridad de la información.
- Concienciación y Capacitación: Fomenta la capacitación y concienciación de los empleados sobre la seguridad de la información y las mejores prácticas para proteger los activos de TI.

2.4 Activos informáticos

ORGANIGRAMA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PARROQUIAL RURAL DE TUFIÑO

- **Área Administrativa**

  Recursos Tecnológicos:

  –1 computadora de escritorio.

  Sistema contable.

  –Servidor que centraliza los servicios tecnológicos.

  –Rack con 12 puntos de red que distribuye la conectividad.

  –10 Thin Clients conectados al servidor para tareas operativas básicas.

  Funciones:

  Gestión contable y administrativa. Soporte a las actividades internas del GADP-Tufiño.

- **Área Operativa**

  Recursos Tecnológicos:

  –1 computadora de escritorio.

  –4 computadoras portátiles usadas para actividades en campo y reuniones.

  Funciones:

  Atención a los ciudadanos.

  Ejecución de proyectos y tareas de campo.

- **Sitio Web Institucional**

  Función:

  Publicación de información y servicios en línea para la ciudadanía.

  Administrada de manera indirecta por el personal del GADP-Tufiño.

- **Conexión Tecnológica**

  El servidor está conectado al rack de red, que distribuye la conectividad a los Thin Clients y demás equipos del GADP-Tufiño.

  El sistema contable opera desde el servidor y está disponible en los dispositivos autorizados. El sitio web puede estar alojado externamente y vinculado al flujo informático del GADP-Tufiño. En la Fig. 7, podemos observar el organigrama de la organización.

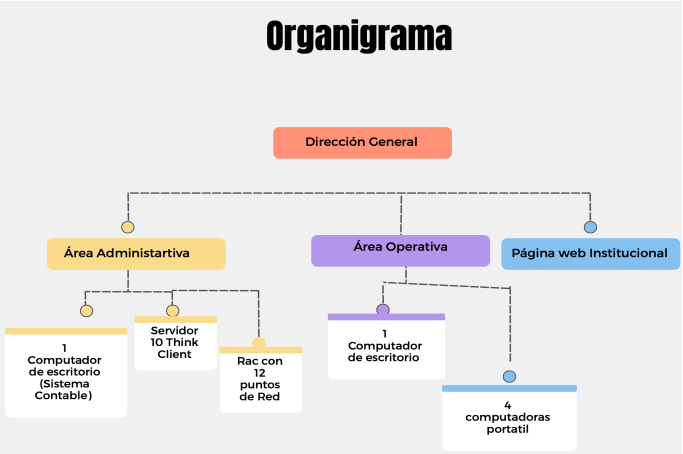


Fig. 7. Organigrama GADP-Tufiño

2.5 Trabajos relacionados

El estudio realizado por Cortés [12], basado en COBIT 2019, evaluó los procesos tecnológicos en la Municipalidad de Carrillo, Guanacaste, Costa Rica, con el objetivo de implementar un modelo de gestión de Tecnologías de Información y Comunicación (TIC) que mejorara las operaciones municipales y detectara brechas respecto a las mejores prácticas de gobernanza y gestión. La aplicación de COBIT 2019 permitió identificar metas y objetivos alineados con sus principios, facilitando la selección de elementos clave a evaluar. Asimismo, se diseñaron herramientas específicas para medir la capacidad y las brechas de cumplimiento, un resumen ejecutivo para comunicar los resultados, y un instrumento gerencial para planificar y monitorear actividades destinadas a cerrar dichas brechas.Estos avances fortalecieron la gestión de TIC de la municipalidad y establecieron una base para evaluaciones futuras, asegurando una mejor alineación con los objetivos de gobernanza institucional.

Según Yohanes Beato Dionisio y Ditdit Nugeraha Utama [8], la Gestión de Continuidad del Negocio (BCM) es un proceso esencial para mitigar riesgos que puedan interrumpir operaciones críticas, asegurando la continuidad operativa y una rápida recuperación tras eventos disruptivos, al tiempo que protege intereses, reputación y servicios esenciales. En el caso de la Lembaga National Single Window (LNSW) de Indonesia, encardo GADP-Tufiño a de gestionar el Sistema de Ventanilla Única Nacional (SINSW), la implementación del BCM fue clave durante la pandemia de COVID-19, debido a la creciente demanda de servicios relacionados con la importación de suministros médicos. Utilizando el marco COBIT 2019, específicamente el dominio DSS04, se evaluó la madurez del BCM en LNSW mediante revisión documental, entrevistas y observación de prácticas. Los resultados mostraron que LNSW alcanzó un nivel parcial de capacidad en la gestión de continuidad, identificándose brechas como la ausencia de un plan integral

de continuidad (BCP), la limitada capacitación del personal y la falta de comunicación interna efectiva sobre la BCM. Estas áreas requieren mejoras para fortalecer la resiliencia operativa.

El estudio de Chimborazo [23], evidenció que los Gobiernos Autónomos Descentralizados (GADP-Tufiños) municipales de Cañar, El Tambo y Suscal no cuentan con un modelo definido de gobierno de Tecnologías de la Información (TI) respaldado en un marco de referencia, lo que limita su capacidad para alinear la estrategia tecnológica con las necesidades locales y optimizar la gestión estratégica de sus servicios, si bien se ha dado prioridad a la migración de sistemas informáticos y se registran avances en aspectos como la gestión del riesgo y la seguridad de la información, persisten desafíos relevantes, como la escasez de personal técnico especializado, en consecuencia, se concluye que resulta indispensable adoptar un modelo de gobierno y gestión de TI enfocado en las necesidades concretas de los GADP-Tufiños, que permita evaluar el desempeño de sus procesos y alinearlos con los objetivos institucionales, con el fin de fortalecer su capacidad de respuesta y mejorar la eficiencia en la prestación de servicios públicos.

El estudio de Tipan [40], analizó las deficiencias en la infraestructura crítica y las políticas de seguridad cibernética de la Corporación Nacional de Telecomunicaciones (CNT) en Ecuador, destacando la baja resiliencia de su infraestructura de internet. Para abordar estos problemas, se desarrolló un modelo de ciberseguridad alineado con el marco NIST v1.1 y COBIT 2019, utilizando la norma NIST 800-30 para identificar y analizar riesgos, garantizando la integridad, disponibilidad y confidencialidad de la información. El proyecto identificó seis objetivos de gobierno y gestión alineados con las necesidades de la alta dirección de la CNT, determinando que su nivel de ciberseguridad estaba en un estado de riesgo informado". Asimismo, se diseñaron 21 proyectos de "quick wins"de bajo costo para optimizar rápidamente los procesos de ciberseguridad. Este enfoque estructurado permitió identificar vulnerabilidades y amenazas específicas, estableciendo un marco para la mejora continua en la gestión de riesgos cibernéticos y generando valor a través de un gobierno efectivo de la ciberseguridad.

Según Haay, Melkior y Sitokdana [4], el estudio sobre la gobernanza de TI en el Servicio de Comunicación e Informática (Diskominfo) de la Provincia de Papua, Indonesia, utilizó COBIT 2019 en el dominio MEA (Monitor, Evaluate and Assess) para evaluar la alineación entre objetivos empresariales y de TI. Los resultados indicaron que el subdominio MEA01, enfocado en la gestión del rendimiento y conformidad, alcanzó un nivel de capacidad de 4, mientras que MEA02, relacionado con el sistema de control interno, obtuvo un nivel de 3, evidenciando avances pero también áreas de mejora. El estudio destacó la necesidad de alinear los objetivos de TI

con los empresariales para garantizar que las iniciativas tecnológicas contribuyan eficazmente a los resultados organizacionales, identificando brechas específicas para optimizar la gobernanza de TI.

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1 Tipo de Investigación

Según Sánchez-García [41]: El modelo de madurez en ciberseguridad tiene varios propósitos prácticos inmediatos que se interrelacionan, en primer lugar, permite a las organizaciones evaluar su estado actual y establecer objetivos y prioridades para la mejora continua, además, ayuda a identificar las capacidades necesarias para alcanzar un estado de madurez deseado, facilitando así el progreso organizativo, en conjunto, estos propósitos contribuyen a implementar estrategias efectivas de seguridad cibernética y a mantener un enfoque en la mejora constante.

3.2 Metodología

La presente investigación se desarrolló bajo un enfoque mixto, integrando métodos cualitativos y cuantitativos, con el propósito de evaluar el nivel de madurez en seguridad informática y formular propuestas de mejora para el GADP-Tufiño, como marco de referencia, se empleó COBIT 2019, el cual proporciona lineamientos estructurados para la gobernanza y gestión de las tecnologías de información, particularmente en el ámbito de la seguridad.

Enfoque Cualitativo

Desde la perspectiva cualitativa, se aplicaron técnicas como el análisis documental, la observación directa y la recolección de información mediante encuestas con preguntas abiertas, estas herramientas permitieron una comprensión profunda del entorno organizacional, la cultura institucional y las prácticas actuales relacionadas con la seguridad de la información.

Los datos obtenidos mediante estas técnicas cualitativas fueron procesados y analizados de forma interpretativa, y constituyeron la base fundamental para el desarrollo del enfoque cualitativo de la investigación, esto facilitó la identificación de brechas, debilidades y oportunidades de mejora, proporcionando una visión integral del estado actual de los procesos y permitiendo contextualizar los hallazgos cuantitativos dentro de la realidad institucional.

Enfoque Cuantitativo

De manera complementaria, se implementó un enfoque cuantitativo a través de la aplicación de encuestas estructuradas, cuyo objetivo fue medir la percepción del personal respecto a la efectividad de los controles de seguridad, así como la alineación de los procesos de TI con los objetivos estratégicos de la organización, los datos recopilados fueron codificados, tabulados

y analizados estadísticamente para sustentar los hallazgos cualitativos con una base objetiva y cuantificable.

3.3 Variables de Estudio

Considerando que son aspecto clave donde mediremos y analizaremos la evaluación de seguridad de TI en el GADP-Tufiño, basado en COBIT 2019, se ha considerado las siguientes variables.

Variable Independiente:

- Madurez de la Seguridad de TI en la organización, evaluada a través del Modelo de Capacidad de COBIT 2019 en los procesos seleccionados (APO01, APO03, APO12, APO13, DSS05).

Variables Dependiente

- Seguridad de la información.
- Integridad de activos.
- Controles de acceso.

3.4 Matriz de Consistencia

A continuación en la tabla I se muestra la matriz de consistencia del estudio.

Tabla I.

MATRIZ DE CONSISTENCIA

Problema general	**Objetivo general**	**Variables**	**Diseño Metodológico**	**Población y muestra**
¿Cuál es el nivel de madurez de la seguridad informática en el Gobierno Autónomo Descentralizado Parroquial Rural de Tufiño y qué mejoras se pueden proponer basándose en COBIT 2019?	Realizar una evaluación de la madurez de seguridad informática y propuesta de mejoras para un Gobierno Autónomo Descentralizado Parroquial Rural de Tufiño: una aproximación basada en COBIT 2019.	**Variable Independiente:** Madurez de la Seguridad de TI **Variable Dependiente:** - Seguridad de la información. - Integridad de activos.	**Enfoque:** Cualitativo Cuantitativo **Tipo de Investigación:** Aplicada **Nivel de Investigación:** Descriptivo	**Población:** La población está conformada por aproximadamente 1.500 habitantes de la parroquia Tufiño, de los cuales se consideró al personal clave que tiene autorización para utilizar el software del GADP-Tufiño. **Muestra:** Se utilizó un muestreo por conveniencia, tomando en cuenta al personal clave relacionado directamente con el uso del software institucional. **Instrumento:** Encuesta estructurada.

3.5 Diagrama de Proceso

En la Fig. 8 se detalla la conclusión basada en COBIT 2019 con enfoque de mejora continua.

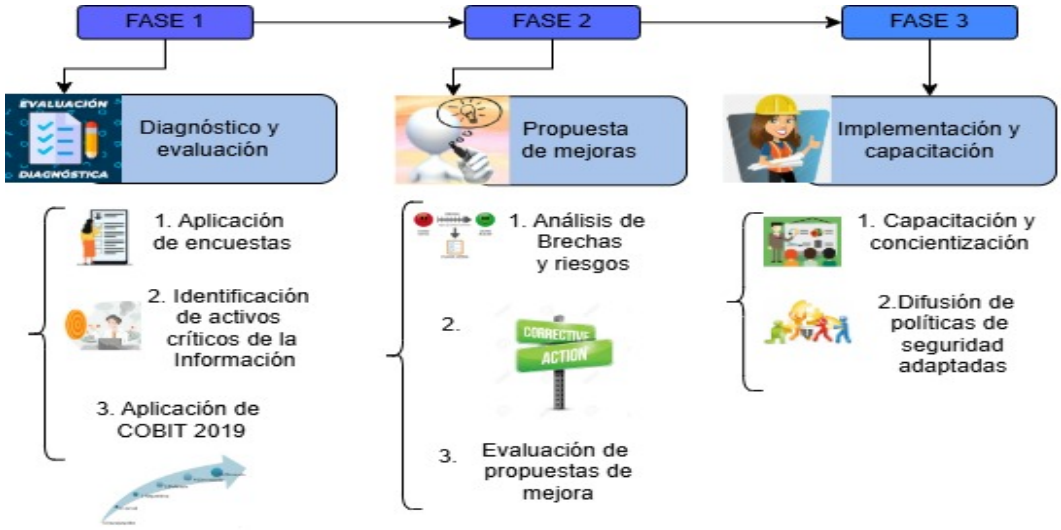


Fig. 8. Diagrama de proceso

3.6 Fase 1: Diagnóstico y Evaluación

Para la realización del estudio, se empleó la observación directa, lo que permitió analizar cómo se aplican las políticas y controles de seguridad basados en COBIT 2019 en la práctica diaria, enfocados en los siguientes dominios clave:

- Gestión de riesgos de TI (APO12).
- Uso de contraseñas seguras y control de accesos (APO13).
- Implementación de herramientas de monitoreo de seguridad (DSS05).
- Gestión de la Arquitectura Empresarial (APO03).
- Gestión del Marco de Gobernanza (APO01).

Además, se aplicaron encuestas a los responsables de los procesos de TI, obteniendo respuestas alineadas con la escala de madurez de COBIT 2019. Entre las actividades realizadas se incluyen:

a) **Evaluación de documentación y políticas existentes.**

- **Estado actual:** El GADP-Tufiño no cuenta con documentación formalizada ni políticas específicas relacionadas con el uso, gestión y mantenimiento de la infraestructura tecnológica.

- **Implicaciones:** La ausencia de lineamientos puede derivar en un uso inadecuado o inseguro de los recursos tecnológicos, no existen políticas de respaldo, seguridad, mantenimiento preventivo ni asignación de equipos. Esta falta de documentación limita el control, la auditoría y la planificación de actualizaciones o renovaciones tecnológicas.

b) **Recolección de información.**

La presente sección describe el proceso seguido para la obtención de información técnica y administrativa, utilizada como base para el diagnóstico institucional y la formulación de acciones correctivas.

Se recolectaron datos orientados a identificar el estado actual de los recursos tecnológicos, las prácticas de seguridad, el nivel de madurez de los procesos y el cumplimiento de medidas clave de protección. Las fuentes consultadas incluyeron:

- Encuestas dirigidas al personal clave.
- Revisión documental de políticas, registros y herramientas institucionales.
- Inventario físico y lógico de los recursos tecnológicos disponibles.
- Escaneos técnicos de seguridad mediante herramientas como Nmap.
- Evaluaciones de madurez conforme a los criterios del modelo COBIT 2019.

Este proceso permitió identificar deficiencias, riesgos y oportunidades de mejora fundamentales para sustentar la propuesta técnica posterior, como lo podemos observar en la tabla II.

Tabla II.
INVENTARIO DE RECURSOS, OBSERVACIONES CRÍTICAS Y RECOMENDACIONES

N°	Tipo de Recurso	Observación Crítica	Riesgo Detectado	Recomendación
1	Sistema contable	Uso en portátiles asignadas sin control individualizado	Acceso débil y no trazable	Implementar autenticación individual por usuario

Cuadro II– *continuación*

N°	Tipo de Recurso	Observación Crítica	Riesgo Detectado	Recomendación
5	Thin Client (10 terminales)	Uso compartido por múltiples usuarios	Falta de trazabilidad de acceso	Establecer control de sesiones y auditoría
7	Laptop	Equipos portátiles fuera de políticas de dominio y cifrado	Exposición a pérdida de datos si no están cifrados o protegidos	Aplicar cifrado, autenticación y políticas móviles
8	Sitio web institucional	Servicio de hosting externo sin especificaciones técnicas conocidas	Riesgo elevado por fallos en la infraestructura	Solicitar documentación del servicio contratado y activar monitoreo continuo

Recomendaciones Inmediatas

a) **Sistema contable y Thin Clients:**

- Verificar que el acceso se realice con usuarios individualizados y autenticación segura.
- Asegurar que los datos estén cifrados en tránsito y que exista trazabilidad de accesos.

b) **Laptops:**

- Confirmar la presencia de antivirus, cifrado de disco y políticas de bloqueo automático.
- Establecer un inventario actualizado y realizar revisiones periódicas de uso.

c) **Sitio web institucional:**

- Solicitar documentación del servicio de hosting externo, incluyendo proveedor, ubicación de los datos y políticas de respaldo.
- Establecer mecanismos básicos de monitoreo y realizar revisiones de seguridad ante posibles vulnerabilidades.

3.7 Aplicación de Encuesta

Encuestas a personal clave.

En el marco de la evaluación de madurez de los procesos de TI, se llevó a cabo una encuesta en el GADP-Tufiño con el objetivo de determinar el nivel de madurez en la gestión de TI, seguridad de la información y procesos tecnológicos.

Para esta evaluación, se aplicó el Modelo de Capacidad de COBIT 2019, asignando valores numéricos a las respuestas de la encuesta en función a la tabla III.

Tabla III.
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.

La encuesta fue aplicada a tres actores clave dentro del GADP-Tufiño:

- Secretario – Representante administrativo del GADP-Tufiño
- Presidente del GADP-Tufiño Responsable de la toma de decisiones estratégicas.
- Responsable de TI – Encardo GADP-Tufiño de la infraestructura y gestión tecnológica.

Los resultados obtenidos permitirán identificar brechas en la madurez de los procesos de TI y formular un plan de mejora basado en COBIT 2019. Cada uno respondió 15 preguntas relacionadas con políticas de TI, gestión de seguridad, monitoreo y auditoría de procesos tecnológicos. Las preguntas realizadas están enfocadas en cada uno de los dominios utilizados: APO01, APO03, APO12, APO13 y DSS05, como se muestra en la tabla IV.

Tabla IV.
PREGUNTAS RELACIONADAS CON LA GESTIÓN DE TI SEGÚN COBIT 2019

	PREGUNTAS	**COBIT 2019**
1	¿Existen políticas formales para la gestión de TI en la organización?	APO01
2	¿Se revisan y actualizan regularmente las políticas de TI?	APO01
3	¿Se han definido claramente los roles y responsabilidades en TI?	APO01
4	¿La infraestructura tecnológica está documentada y planificada?	APO03
5	¿Se siguen estándares de arquitectura tecnológica en la institución?	APO03
6	¿Existen políticas para la actualización y mantenimiento de la infraestructura?	APO03
7	¿Se han identificado los principales riesgos de seguridad en TI?	APO12
8	¿Existe un proceso formal para evaluar y mitigar los riesgos de TI?	APO12
9	¿Se realizan auditorías de riesgos periódicamente?	APO12
10	¿Se cuenta con normativas de seguridad alineadas a estándares internacionales?	APO13
11	¿Existen controles de acceso a la información y sistemas?	APO13
12	¿Se capacita al personal en seguridad de la información?	APO13
13	¿Se realiza monitoreo continuo de los servicios de TI?	DSS05
14	¿Se han implementado herramientas para detectar amenazas y vulnerabilidades?	DSS05
15	¿Existe un plan de respuesta ante incidentes de seguridad?	DSS05

La encuesta fue contestada de la siguiente manera:

En la Fig. 9 se muestra la respuesta a la pregunta 1:

¿Existen políticas formales para la gestión de TI en la organización?

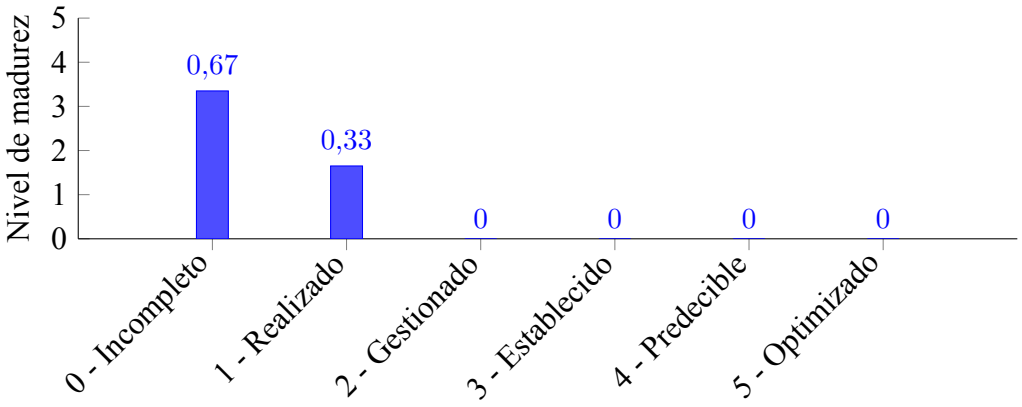


Fig. 9. Google Forms: ¿Existen políticas formales para la gestión de TI?

- La mayoría de los encuestados (2 de 3) evaluaron que no existen políticas formales para la gestión de TI, ubicando a la organización en el nivel 0 - Incompleto. Esto significa

que la organización no cuenta con lineamientos claros, documentados ni aplicados para la gestión de tecnología de la información.

- Una sola respuesta (33.3 %) indica que está en el nivel 1 - Realizado, lo cual implica que aunque existen ciertas prácticas aisladas, estas no están formalizadas ni institucionalizadas.

Interpretación:

a) Predominio de respuestas en nivel 0 indica que:

   - No existen políticas formales establecidas. No hay un enfoque sistemático o documentado para la gestión de TI.
   - Es muy probable que se gestionen aspectos de TI de forma ad hoc o no se gestionen.

b) El 33.3 % que marca nivel 1 (Realizado):

   - Reconoce al menos un inicio o intento de formalización.
   - Sin embargo, no cumple con los criterios de madurez mínimos exigidos por COBIT (nivel 3).

La pregunta 1 evidencia una brecha crítica en la formalización de políticas de TI, la mayoría de los evaluadores percibe que la organización no tiene políticas formales para la gestión de TI, esto representa un riesgo importante en cuanto a gobernanza tecnológica, cumplimiento y alineación estratégica.

Fig. 10 se muestra la respuesta a la pregunta 2:

¿Se revisan y actualizan regularmente las políticas de TI?

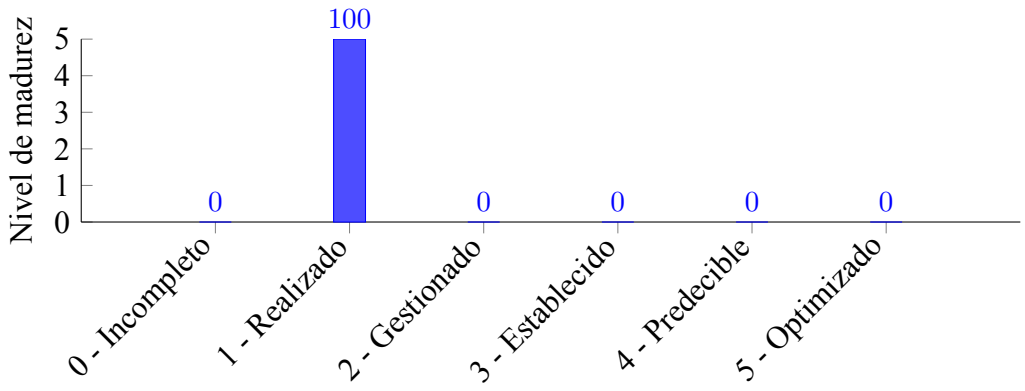


Fig. 10. Google froms: ¿Se revisan y actualizan regularmente las políticas de TI?

Distribución de respuestas:

- 100 % de las respuestas (3 de 3) están en el nivel 1 - Realizado.
- 0 % en nivel 0 (incompleto).
- 0 % en niveles 2 o superiores (ningún avance en madurez formal).

Interpretación:

a) Nivel 1 – Realizado (100 %):

- Indica que existe alguna revisión o actualización, pero de forma informal o no estandarizada.
- Puede depender de personas o de situaciones reactivas.
- No hay evidencia de planificación, controles, documentación ni mejora continua.

b) Ausencia de niveles 2 a 5:

Refleja que no se han establecido mecanismos sistemáticos, ni procedimientos formales, ni indicadores de desempeño para esta práctica.

Fig. 11 se muestra la respuesta a la pregunta 3:

¿Se han definido claramente los roles y responsabilidades en TI?

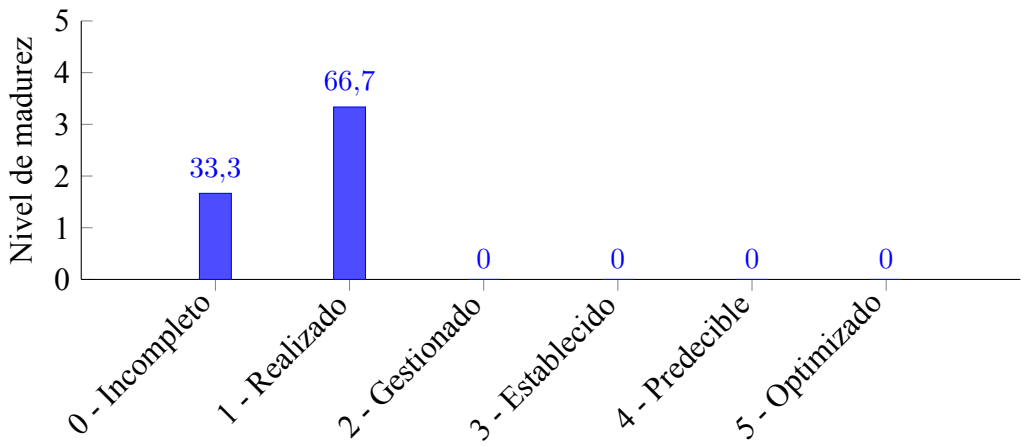


Fig. 11. Google Forms: ¿Existen políticas formales para la gestión de TI?

Distribución de respuestas:

- 66.7 % (2 de 3) marcaron nivel 1 - Realizado
- 33.3 % (1 de 3) marcaron nivel 0 - Incompleto
- 0 % alcanzó niveles 2 a 5 (ningún avance formal)

Interpretación:

a) La mayoría considera que hay un reconocimiento o definición parcial de roles y responsabilidades en TI.

   - Esto podría significar que algunos roles existen de facto, pero no están formalmente documentados o asignados.

b) Un tercio aún considera que no hay ninguna definición (nivel 0), lo que indica falta de consenso institucional o inexistencia total en algunos casos.

c) Ausencia total de niveles 2 a 5:

   - No se evidencia que existan estructuras organizativas formalizadas, políticas aprobadas o mecanismos de control relacionados con funciones en TI.

La organización aún no ha alcanzado un nivel mínimo de madurez en cuanto a la definición de roles y responsabilidades en el área de TI, aunque existe cierto grado de identificación, falta estandarización, documentación y oficialización, lo que genera ambigüedades en funciones y toma de decisiones.

Fig. 12 se muestra la respuesta a la pregunta 4:

¿Se han definido claramente los roles y responsabilidades en TI?

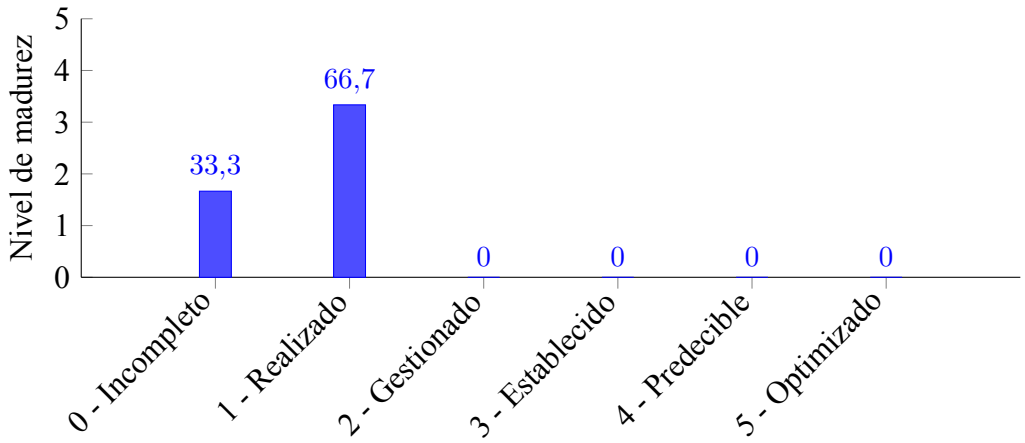


Fig. 12. Google Forms: ¿Se han definido claramente los roles?

Distribución de respuestas:

- 66.7 % (2 de 3 respuestas) indicaron nivel 1 - Realizado
- 33.3 % (1 de 3 respuestas) indicaron nivel 0 - Incompleto
- 0 % en niveles 2 a 5 (no hay planificación o documentación formal)

Interpretación:

a) La mayoría de los encuestados considera que existe alguna planificación básica o reconocimiento informal de la infraestructura, aunque sin formalización.

b) La presencia de una respuesta en nivel 0 indica que al menos una persona percibe una falta total de documentación o planificación estructurada.

c) No hay evidencia de:

- Inventarios actualizados
- Diagramas de red
- Documentación de servidores, cableado o topología
- Políticas de renovación o gestión de activos

La organización presenta un estado inicial de planificación tecnológica, con prácticas informales que aún no cumplen los requisitos mínimos del modelo COBIT 2019.

Fig. 13 se muestra la respuesta a la pregunta 5:

¿Se siguen estándares de arquitectura tecnológica en la institución?

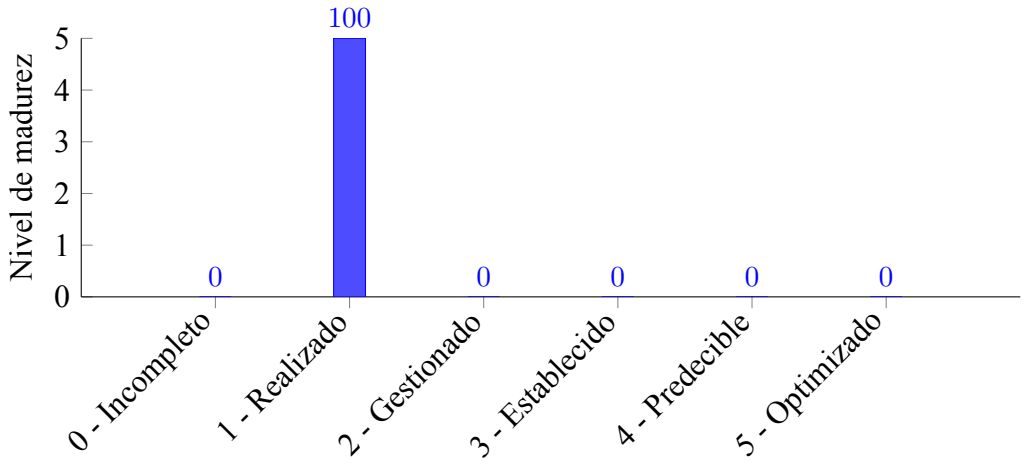


Fig. 13. Google froms: ¿Se revisan y actualizan regularmente las políticas de TI?

Distribución de respuestas:

- 100 % de las respuestas están en el nivel 1 - Realizado
- 0 % en nivel 0 (nadie considera que está totalmente ausente)
- 0 % en niveles 2 a 5 (no hay evidencia de madurez formal)

Interpretación:

a) Todos los encuestados coinciden en que existe algún grado de seguimiento a estándares de arquitectura.

b) El hecho de que nadie haya seleccionado niveles 2 o superiores implica que:

- No hay una arquitectura empresarial definida.
- No existe una visión común de APO01 y escalabilidad de los sistemas.

Aunque hay conciencia y algunas prácticas en marcha, la institución se encuentra en un estado inicial respecto al uso de estándares de arquitectura tecnológica. Se requiere estructurar, formalizar y documentar una arquitectura alineada a los objetivos estratégicos, incluyendo interoperabilidad y planificación de largo plazo.

Fig. 14 se muestra la respuesta a la pregunta 6:

¿Existen políticas para la actualización y mantenimiento de la infraestructura?

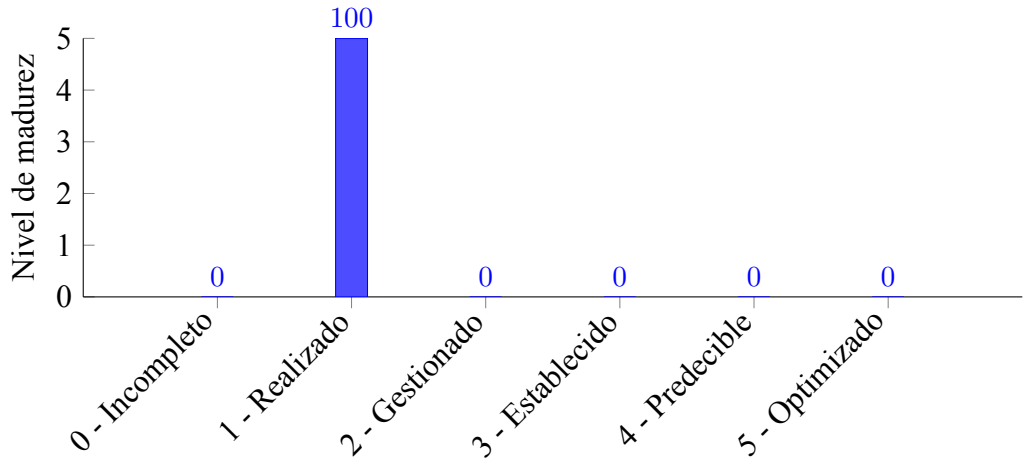


Fig. 14. Google froms: Existen políticas para la actualización y mantenimiento

Distribución de respuestas:

- 100 % de las respuestas están en el nivel 1 - Realizado
- 0 % en nivel 0 (nadie considera que no se hace nada)
- 0 % en niveles 2 a 5 (sin evidencia de madurez estructurada)

Interpretación:

a) La unanimidad en el nivel 1 - Realizado indica que:

- Sí existe actividad de actualización o mantenimiento, pero de forma informal, no planificada ni sistematizada.
- Es probable que las acciones sean reactivas (cuando hay fallas) y no basadas en un plan de mantenimiento preventivo.

b) No hay evidencia de:

- Un plan de mantenimiento aprobado y calendarizado.
- Una política formal de actualización de hardware o software.
- Documentación de mantenimientos realizados.

Aunque existe conciencia sobre la necesidad de actualizar y mantener la infraestructura tecnológica, la institución aún se encuentra en una fase temprana, el nivel alcanzado (1) refleja acciones puntuales sin una estructura de gobernanza clara.

Fig. 15 se muestra la respuesta a la pregunta 7:

¿Se han identificado los principales riesgos de seguridad en TI?

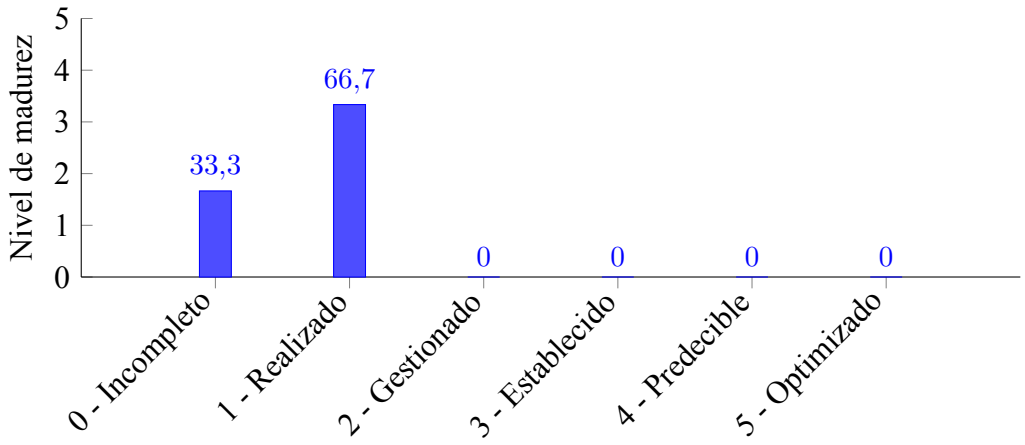


Fig. 15. Google Forms: ¿Se han identificado los principales riesgos de seguridad?

Distribución de respuestas:

- 66.7 % (2 de 3) seleccionaron nivel 1 - Realizado
- 33.3 % (1 de 3) seleccionó nivel 0 - Incompleto
- 0 % en niveles 2 a 5 (no hay gestión formal ni sistemática)

Interpretación:

1) La mayoría de respuestas en nivel 1 indica que:

- Hay una identificación básica de riesgos, posiblemente informal o basada en experiencias pasadas.
- No se ha desarrollado un inventario documentado de amenazas ni una evaluación sistemática.

La respuesta en nivel 0 revela que al menos una persona considera que no se identifican riesgos de seguridad en absoluto.

2) La ausencia total de niveles 2, 3, 4 o 5 indica que:

- No se aplica una metodología de gestión de riesgos
- No se documentan ni priorizan riesgos
- No se hace un seguimiento ni revisión periódica de estos riesgos

Aunque se reconoce parcialmente la existencia de riesgos en TI, la organización aún no los identifica formalmente ni los gestiona de forma estructurada, esto deja abierta una importante brecha de seguridad, dado que los riesgos no gestionados pueden materializarse sin que exista un plan de respuesta o mitigación.

Fig. 16 se muestra la respuesta a la pregunta 8:

¿Existe un proceso formal para evaluar y mitigar los riesgos de TI?

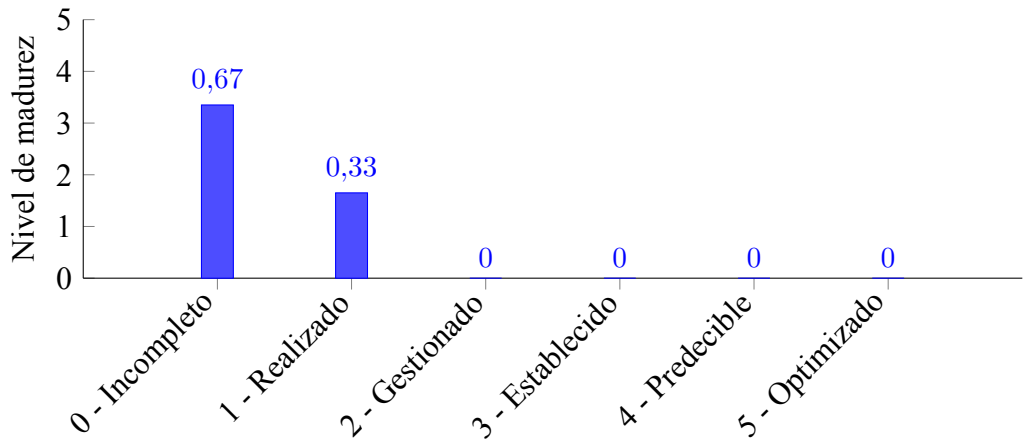


Fig. 16. Google Forms: ¿Existen políticas formales para la gestión de TI?

Distribución de respuestas:

- 66.7 % (2 de 3) respondieron nivel 0 - Incompleto
- 33.3 % (1 de 3) respondió nivel 1 - Realizado
- 0 % en niveles 2 a 5 (sin madurez formal)

Interpretación:

a) La mayoría considera que no existe un proceso formalizado para la evaluación y mitigación de riesgos de TI.

- Es posible que haya acciones aisladas o conocimiento implícito de algunos riesgos, pero sin planificación ni documentación formal.

b) La respuesta en nivel 1 sugiere que alguna persona considera que se han realizado acciones iniciales, pero sin una metodología estructurada.

c) La ausencia de respuestas en niveles superiores muestra que:

- No se aplican marcos de seguridad.
- No se cuenta con registros de evaluación, clasificación o respuesta a riesgos.
- No se mide el tratamiento de riesgos ni su evolución en el tiempo.

La organización carece de un proceso formal y documentado para gestionar los riesgos de TI, esta situación representa una vulnerabilidad crítica, ya que los riesgos pueden materializarse sin un plan de respuesta, ni asignación de responsables ni priorización basada en impacto.

Fig. 17 se muestra la respuesta a la pregunta 9:

¿Se realizan auditorías de riesgos periódicamente?

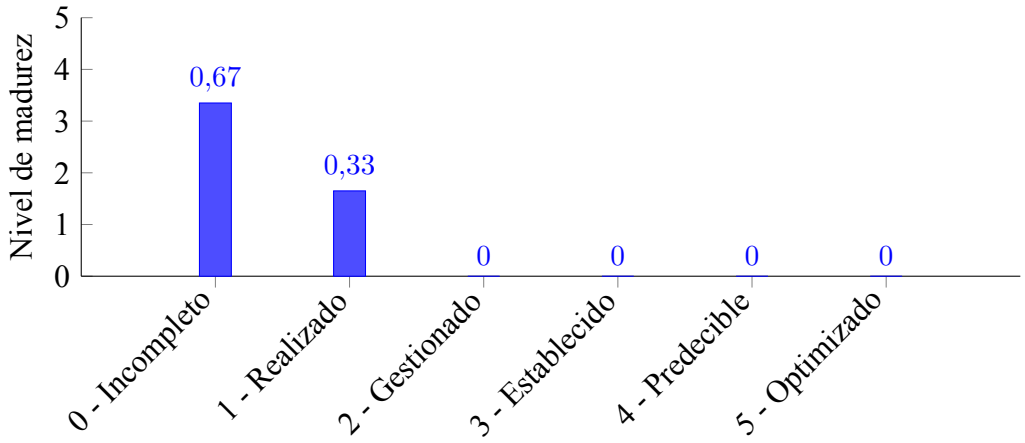


Fig. 17. Google Forms:¿Se realizan auditorías de riesgos periódicamente?

Distribución de respuestas:

- 66.7 % (2 de 3) seleccionaron nivel 0 - Incompleto 33.3 % (1 de 3) seleccionó nivel 1 - Realizado 0 % en niveles 2 a 5 (no existe un enfoque estructurado)

Interpretación:

a) La mayoría de respuestas indican que no se realizan auditorías periódicas de riesgos, o que si se hacen, no están formalizadas ni documentadas.

b) El único 33.3 % en nivel 1 sugiere que puede haber alguna revisión ocasional, pero no sistemática ni basada en estándares.

c) No hay evidencia de:

- Auditorías internas o externas planificadas y documentadas.
- Seguimiento a hallazgos o no conformidades.

La falta de auditorías periódicas de riesgos indica una debilidad crítica en el ciclo de gestión de la seguridad de la información, sin auditoría, no es posible verificar si los riesgos están siendo tratados, si los controles son efectivos o si hay nuevas amenazas emergentes. Esta situación impide avanzar hacia la mejora continua y el cumplimiento normativo.

Fig. 18 se muestra la respuesta a la pregunta 10:

¿Se cuenta con normativas de seguridad alineadas a estándares internacionales?

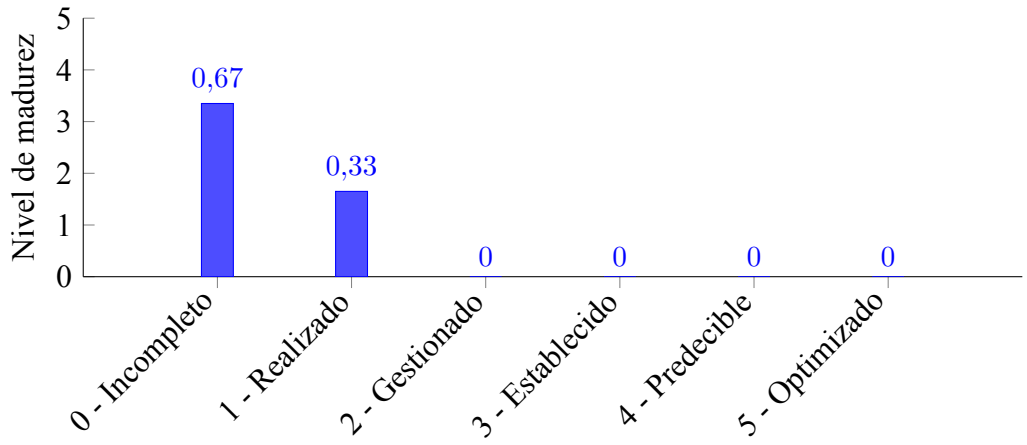


Fig. 18. Google Forms:¿Se cuenta con normativas de seguridad?

Distribución de respuestas:

- 66.7 % (2 de 3) marcaron nivel 0 - Incompleto
- 33.3 % (1 de 3) marcó nivel 1 - Realizado
- 0 % en niveles 2 a 5 (sin cumplimiento estructurado)

Interpretación:

a) Dos de tres encuestados consideran que no existen normativas de seguridad.

b) Una respuesta en nivel 1 sugiere que existe algún conocimiento o iniciativa básica, pero aún informal o sin respaldo documental.

c) La ausencia total en niveles ≥2 implica que:

- No se han adoptado frameworks reconocidos internacionalmente.
- No hay políticas específicas sobre control de accesos, cifrado, gestión de incidentes, etc.
- No se mide ni monitorea el cumplimiento con base en estándares.

La institución aún no cuenta con normativas de seguridad alineadas a estándares internacionales, o estas no están formalizadas, esta carencia expone a la organización a inconsistencias en la protección de la información, falta de control sobre los activos tecnológicos, y débil respuesta ante auditorías externas.

Fig. 19 se muestra la respuesta a la pregunta 11:

¿Existen controles de acceso a la información y sistemas?

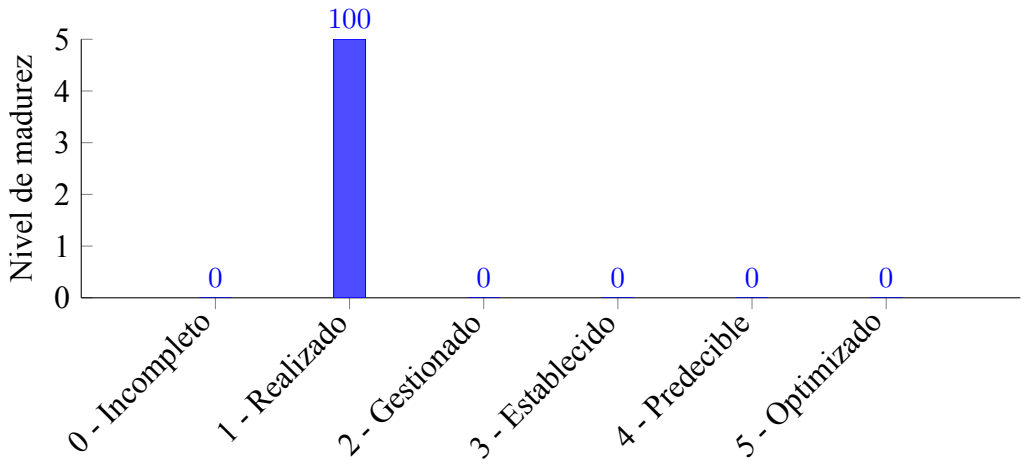


Fig. 19. Google froms: ¿Existen controles de acceso a la información y sistemas?

Distribución de respuestas:

- 100 % de las respuestas (3 de 3) se ubicaron en nivel 1 - Realizado
- 0 % en niveles 0 y superiores a 1

Interpretación:

1) Todos los encuestados reconocen que existen controles de acceso, lo cual es un buen punto de partida.

2) Sin embargo, el hecho de que todos estén solo en nivel 1 indica que:

- Los controles de acceso son básicos, probablemente definidos por usuario/contraseña sin políticas avanzadas.

- No existe un proceso documentado de gestión de accesos (altas, bajas, cambios).
- No hay mecanismos como:
- Revisión periódica de privilegios.
- Auditoría de accesos.

Aunque existen mecanismos de acceso, estos no están formalizados ni alineados a buenas prácticas de seguridad, el uso de controles simples y la falta de gestión estructurada representa un riesgo, especialmente en entornos donde se maneja información sensible.

Fig. 20 se muestra la respuesta a la pregunta 12:

¿Se capacita al personal en seguridad de la información?

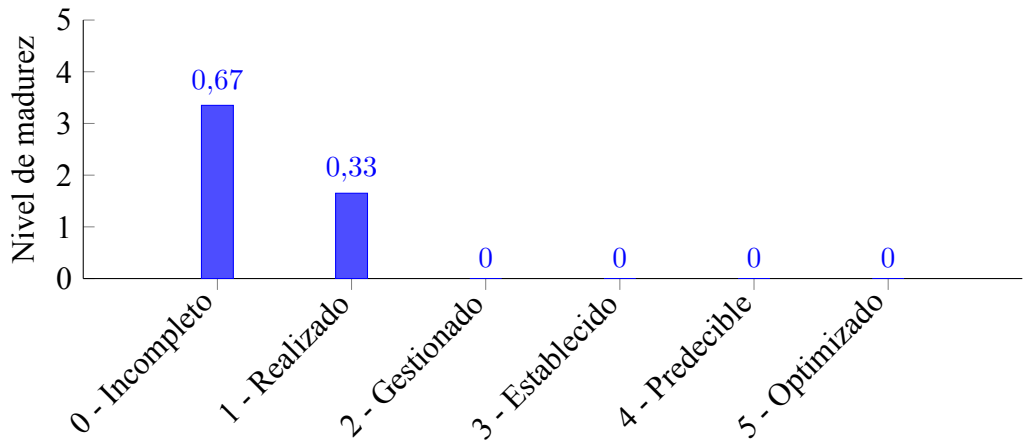


Fig. 20. Google Forms:¿Se capacita al personal en seguridad de la información?

Distribución de respuestas:

- 66.7 % (2 de 3) marcaron nivel 0 - Incompleto
- 33.3 % (1 de 3) marcó nivel 1 - Realizado
- 0 % en niveles 2 a 5

Interpretación:

a) La mayoría considera que no se realiza ningún tipo de capacitación en seguridad de la información.

b) Solo una persona percibe que existe una acción inicial o informal, como una charla o advertencia ocasional.

c) La ausencia total de niveles superiores indica que:

- No se documentan capacitaciones ni se evalúan conocimientos.
- No existe cultura institucional de seguridad digital entre los usuarios.

La capacitación del personal en seguridad de la información es un aspecto críticamente débil dentro de la organización, la falta de formación sistemática expone a la institución a riesgos por errores humanos, como clics en enlaces maliciosos, pérdida de información o incumplimiento normativo.

Fig. 21 se muestra la respuesta a la pregunta 13: **¿Se realiza monitoreo continuo de los servicios de TI?**

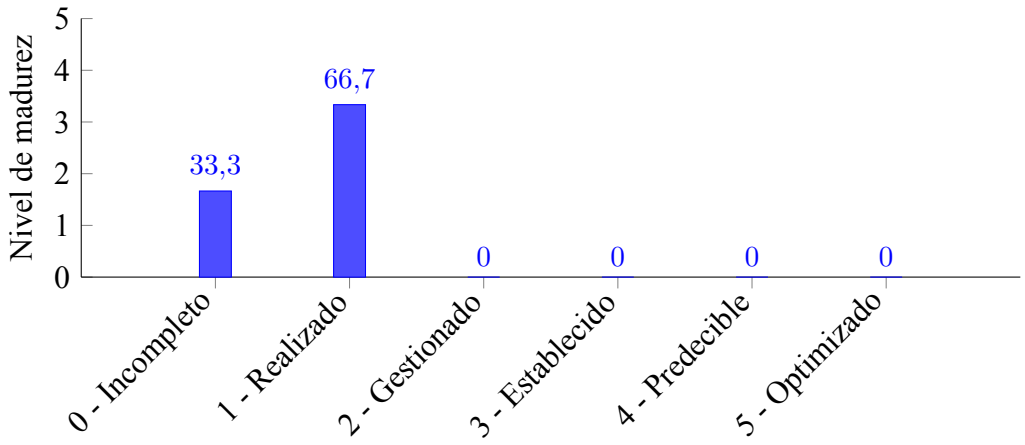


Fig. 21. Google Forms: ¿Se realiza monitoreo continuo de los servicios de TI?

Distribución de respuestas:

- 66.7 % (2 de 3) seleccionaron nivel 1 - Realizado
- 33.3 % (1 de 3) seleccionó nivel 0 - Incompleto
- 0 % en niveles 2 a 5

Interpretación:

a) Dos personas consideran que existe alguna forma de monitoreo inicial o informal, pero sin estructura ni herramientas especializadas.

b) Una persona percibe que no existe ningún monitoreo formal, lo que sugiere falta de visibilidad sobre el rendimiento, disponibilidad o fallos de los servicios TI.

c) La falta de respuestas en niveles 2 a 5 indica que:

- No hay dashboards, alertas automatizadas o registros históricos.

- No se hace seguimiento a indicadores clave de desempeño (KPIs).

Aunque se realiza algún tipo de observación básica sobre los servicios de TI, no existe un monitoreo estructurado, continuo ni preventivo, esta debilidad impide detectar fallos oportunamente, anticiparse a incidentes y garantizar la disponibilidad de los servicios críticos.

Fig. 22 se muestra la respuesta a la pregunta 14:

¿Se han implementado herramientas para detectar amenazas y vulnerabilidades?

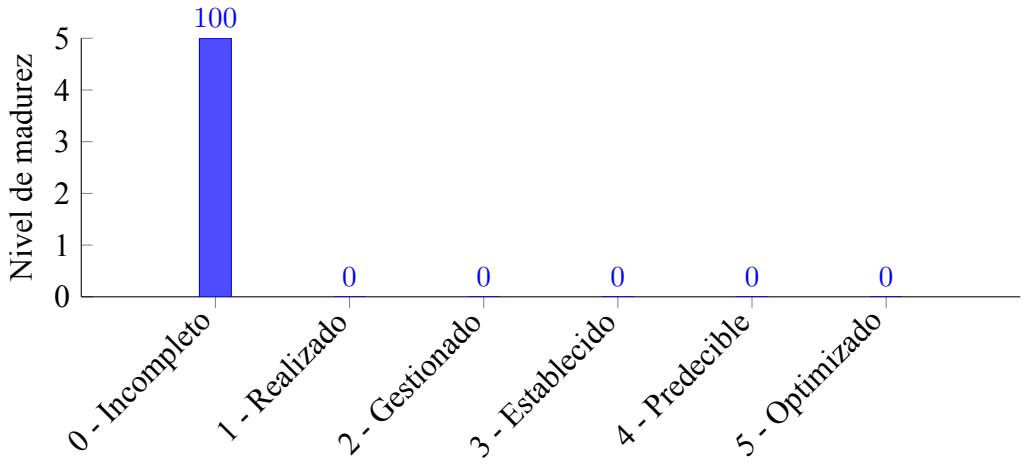


Fig. 22. Google froms: ¿Se han implementado herramientas para detectar amenazas?

Distribución de respuestas:

- 100 % (3 de 3) marcaron nivel 0 - Incompleto
- 0 % en niveles 1 a 5

Interpretación:

a) Todas las respuestas indican que no se han implementado herramientas para la detección de amenazas o vulnerabilidades.

b) Esto implica que:

   - No se utilizan antivirus empresariales centralizados, escáneres de vulnerabilidades (como Nessus, OpenVAS), ni SIEMs (como Splunk, Wazuh).
   - No hay capacidades de análisis preventivo ni monitoreo proactivo.
   - La organización está funcionando sin mecanismos para identificar fallos de seguridad críticos.

Fig. 23 se muestra la respuesta a la pregunta 15:

¿Existe un plan de respuesta ante incidentes de seguridad?

Distribución de respuestas:

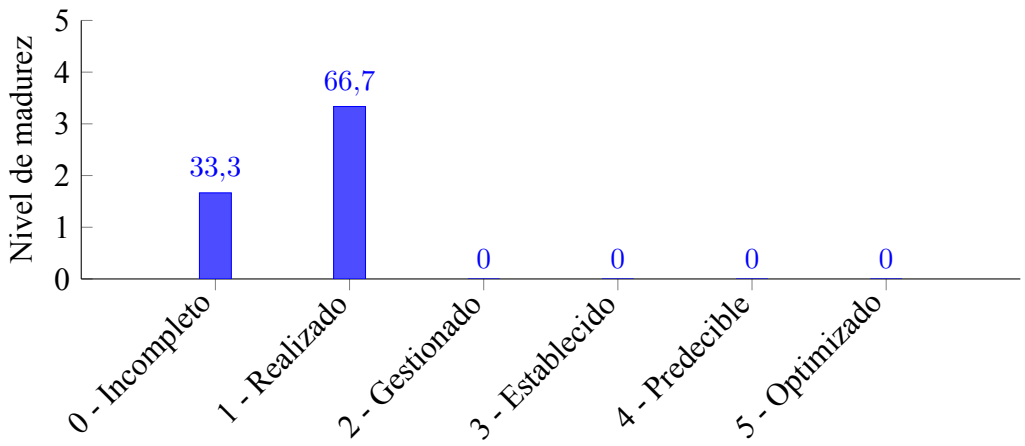


Fig. 23. Google Forms: ¿Existe un plan de respuesta ante incidentes de seguridad?

- 66.7 % (2 de 3 respuestas) marcaron nivel 1 - Realizado
- 33.3 % (1 de 3 respuestas) marcó nivel 0 - Incompleto
- 0 % en niveles 2 a 5

Interpretación:

a) La mayoría indica que existen acciones básicas ante incidentes, pero que no están formalizadas.

b) Una persona considera que ni siquiera existe un plan de respuesta o acciones mínimas establecidas.

c) La ausencia de niveles superiores refleja que:

- No existe un procedimiento documentado y aprobado para gestionar incidentes.
- No hay responsables designados ni flujo definido de actuación.
- No se realizan simulacros ni análisis post-incidente (lecciones aprendidas).
- No se documentan ni reportan formalmente los incidentes.

El nivel actual de madurez en este aspecto es muy bajo, aunque hay acciones puntuales, la falta de un plan estructurado de respuesta a incidentes compromete la capacidad institucional de reaccionar de forma efectiva frente a amenazas reales como ciberataques, pérdida de datos o accesos no autorizados.

Análisis De Madurez

Puntaje Promedio: La mayoría de las respuestas se ubican en los niveles.

- 0 (Incompleto)

- 1 (Realizado)

La tabla V, indica que la gestión de TI está en una fase inicial, con falta de documentación, procesos estructurados y auditorías formales. Las respuestas contienen puntuaciones categorizadas como 0 - Incompleto y 1 - Realizado. Para calcular el nivel de madurez promedio, se convirtieron estas respuestas en valores numéricos y se aplicó el nivel promedio de las preguntas contestadas.

Tabla V.
CÁLCULO DE LA MADUREZ PROMEDIO

Pregunta	**Cumplido (valor 1)**	**Total respuestas**	**% de cumplimiento**
1.- ¿Existen políticas formales para la gestión de TI en la organización?	1	3	33.33 %
2.- ¿Se revisan y actualizan regularmente las políticas de TI?	3	3	100.0 %
3.- ¿Se han definido claramente los roles y responsabilidades en TI?	2	3	66.67 %
4.- ¿La infraestructura tecnológica está documentada y planificada?	2	3	66.67 %
5.- ¿Se siguen estándares de arquitectura tecnológica en la institución?	3	3	100.0 %
6.- ¿Existen políticas para la actualización y mantenimiento de la infraestructura?	3	3	100.0 %
7.- ¿Se han identificado los principales riesgos de seguridad en TI?	2	3	66.67 %
8.- ¿Existe un proceso formal para evaluar y mitigar los riesgos de TI?	1	3	33.33 %
9.- ¿Se realizan auditorías de riesgos periódicamente?	1	3	33.33 %
10.- ¿Se cuenta con normativas de seguridad alineadas a estándares internacionales?	1	3	33.33 %

Pregunta	Cumplido (valor 1)	Total respuestas	% de cumplimiento
11.- ¿Existen controles de acceso a la información y sistemas?	1	3	33.33 %
12.- ¿Se capacita al personal en seguridad de la información?	1	3	33.33 %
13.- ¿Se realiza monitoreo continuo de los servicios de TI?	2	3	66.67 %
14.- ¿Se han implementado herramientas para detectar amenazas y vulnerabilidades?	0	3	0 %
15.- ¿Existe un plan de respuesta ante incidentes de seguridad?	2	3	66.67 %

Aunque ciertos ítems fueron parcialmente cumplidos (valorados en 1), de acuerdo al modelo COBIT 2019, no se alcanza un nivel de madurez válido mientras las respuestas no superen el umbral de nivel 3.

En la tabla VI, se demuestra que hay una pregunta en la que todos respondieron con 0.

Tabla VI.

PREGUNTAS MENOS CUMPLIDAS

Pregunta	% Cumplimiento
14.- ¿Se han implementado herramientas para detectar amenazas y vulnerabilidades?	0 %
1, 8, 9, 10	33.33 % cada una

La pregunta 14 no fue cumplida por ningún proceso evaluado representa una brecha crítica inmediata.

- Pregunta 1 – Políticas formales para gestión
- Pregunta 8 – Evaluación formal de seguridad
- Pregunta 9 – Auditorías periódicas

- Pregunta 10 – Normativas de seguridad

Estas preguntas tienen señales de avance y podrían priorizarse para reforzar, las acciones correctivas primero en las preguntas con 0 % de cumplimiento (como la 14).
Paralelamente, reforzar las de cumplimiento parcial (33.33 %) para llevarlas a cumplimiento completo.
Como se muestra en la Fig. 24, las áreas críticas presentan un bajo nivel de madurez (0 – Incompleto).

- No hay un proceso formal para mitigar riesgos de TI.
- No se realizan auditorías de riesgos periódicas.
- No se han implementado herramientas para detección de amenazas y vulnerabilidades.

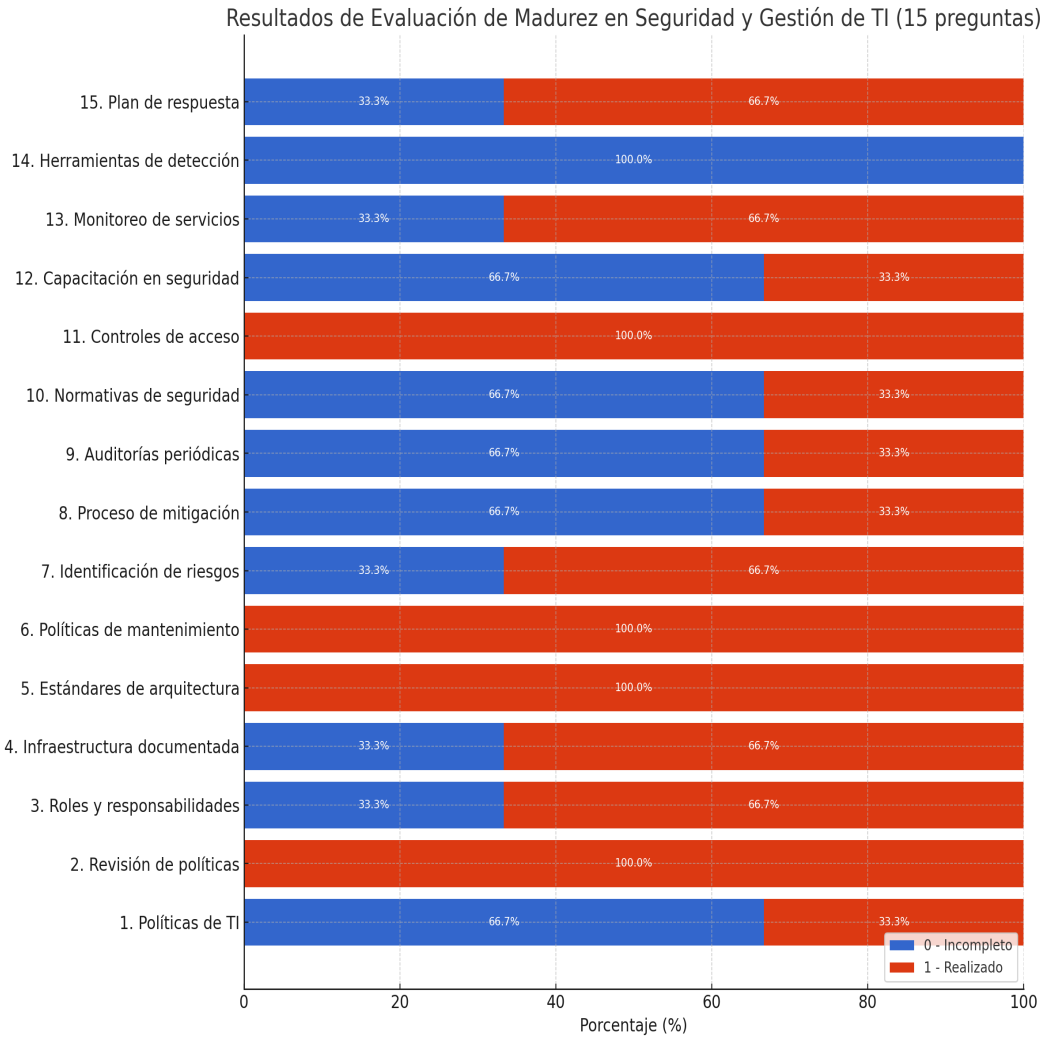


Fig. 24. Áreas críticas con bajo nivel de madurez (0 – Incompleto).

3.8 Tabla de Consolidación de Resultados – Encuesta COBIT 2019

En la siguiente tabla VII se resumen los niveles de madurez promedio por proceso evaluado con base en las respuestas recopiladas en una escala de 0 a 5 utilizando el Modelo de Capacidad de COBIT 2019, donde se incluyen observaciones que indican el estado actual del proceso y recomendaciones generales de mejora.

Tabla VII.
NIVELES DE MADUREZ PROMEDIO POR PROCESO COBIT 2019

Proceso COBIT	Nivel de Madurez Promedio	Observaciones
APO01	0.67	Nivel bajo. Requiere intervención urgente para establecer políticas básicas.
APO03	0.89	Nivel bajo. Requiere intervención urgente para establecer políticas básicas.
APO12	0.44	Nivel bajo. Requiere intervención urgente para establecer políticas básicas.
APO13	0.56	Nivel bajo. Requiere intervención urgente para establecer políticas básicas.
DSS05	0.44	Nivel bajo. Requiere intervención urgente para establecer políticas básicas.

A continuación, la Fig. 25 muestra el nivel de madurez actual.

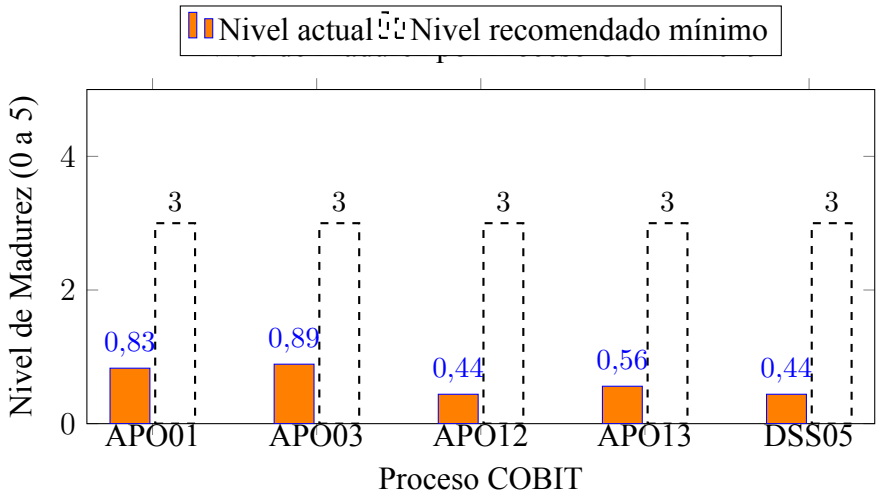


Fig. 25.. Nivel de madurez por proceso COBIT 2019.

Factores de Diseño en COBIT 2019

COBIT 2019 define once Factores de Diseño (DF) que influyen directamente en cómo debe ser diseñado un sistema de gobierno de TI para una organización [29], como se muestra en la tabla VIII.

Tabla VIII.
FACTORES DE DISEÑO SEGÚN COBIT 2019

Código	Nombre del Factor de Diseño	Descripción
DF1	Estrategia empresarial	Define si la estrategia de la organización es tradicional, digital o híbrida.
DF2	Metas empresariales	Refleja las metas específicas que la empresa desea alcanzar con el uso de TI.
DF3	Perfil de riesgo	Evalúa la exposición al riesgo tecnológico de la organización.
DF4	Problemas actuales relacionados con I&T	Considera los problemas que enfrenta la organización con sus sistemas tecnológicos.
DF5	Escenario de amenazas	Nivel de exposición de la organización a amenazas tecnológicas internas y externas.
DF6	Requisitos de cumplimiento	Obligaciones legales, regulatorias o contractuales relacionadas con TI.
DF7	Rol de TI	Rol que desempeña TI en la organización: soporte, fábrica o estratégica.
DF8	Modelo de abastecimiento de servicios de TI	Define si los servicios TI se gestionan internamente, externamente o de forma mixta.
DF9	Métodos de implementación	Enfoques preferidos para implementar cambios o proyectos relacionados con TI.
DF10	Estrategia de adopción tecnológica	Nivel de apertura de la organización a la adopción de nuevas tecnologías.
DF11	Tamaño de la organización	Afecta el alcance y la complejidad del sistema de gobierno de TI.

Evaluación de Factores de Diseño según COBIT 2019

La tabla IX presenta la evaluación de los factores de diseño propuestos por COBIT 2019.

Tabla IX.
EVALUACIÓN DE LOS FACTORES DE DISEÑO SEGÚN COBIT 2019

Factor de Diseño	Descripción Resumida	Evaluación	Justificación
Estrategia empresarial	¿Es impulsada por TI? ¿Tradicional? ¿Digital?	Alto	El GADP-Tufiño busca digitalizar servicios administrativos
Metas empresariales	¿Qué metas TI deben alcanzarse?	Alto	Se requiere eficiencia en servicios y transparencia ciudadana

Cuadro IX– *continuación*

Factor de Diseño	**Descripción Resumida**	**Evaluación**	**Justificación**
Perfil de riesgo	¿Existen riesgos altos en seguridad y continuidad?	Alto	Infraestructura TI limitada y con vulnerabilidades
Problemas actuales relacionados con I&T	¿Qué dificultades presenta hoy la TI?	Alto	Falta de controles, documentación y respuesta a incidentes
Requisitos de cumplimiento	¿Hay leyes o normas que obligan a gestionar TI?	Medio	Se aplican leyes de protección de datos
Rol de TI	¿TI tiene un rol de soporte o es estratégica?	Medio	TI da soporte, pero no se involucra en decisiones estratégicas
Modelo de abastecimiento de servicios de TI	¿Interno, tercerizado o mixto?	Bajo	La gestión TI es interna con muy pocos proveedores externos
Métodos de implementación	¿Cómo suelen abordarse los proyectos?	Medio	No hay una metodología formal definida
Estrategia de adopción tecnológica	¿Se adoptan nuevas tecnologías con frecuencia?	Bajo	Poca adopción de herramientas innovadoras
Tamaño de la empresa	¿Influye en la complejidad de implementación?	Medio	GADP-Tufiño pequeño, pero con responsabilidad institucional creciente

Aplicando al contexto del GADP-Tufiño Parroquial Rural de Tufiño, esta evaluación permite determinar cuáles procesos del marco deben ser priorizados para su implementación, considerando el entorno institucional, los objetivos estratégicos y los riesgos identificados.

Como resultado de esta evaluación, se identifican como factores críticos la estrategia empresarial, el perfil de riesgo y los problemas actuales relacionados con la tecnología de la información. Por 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 El GADP-Tufiño, como se detalla en la tabla X.

Tabla X.
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

Prioridad de Objetivos según Escenario de Amenazas – COBIT 2019

Se consideran las estructuras organizativas, funciones de seguridad y aspectos culturales necesarios para afrontar los niveles de exposición a amenazas tecnológicas.Además, se considera el Valor del factor de diseño, detalles importantes como la prioridad de los objetivos de gobierno y gestión, componentes que detallan cada una de sus estructuras organizativas y las variantes del área prioritaria que son factores importantes para haber elegido los dominios seleccionados,este enfoque permite adaptar el sistema de gobernanza y gestión a las necesidades reales de la organización frente a amenazas internas y externas.

En la tabla XI, se puede observar la alineación con las metas de gobierno, que garantiza una toma de decisiones informada, basada en riesgos y en el cumplimiento normativo. Cada uno de los puntos tomados en cuenta es esencial para el buen desarrollo de la determinación de la madurez.

Complemento de Factores de Diseño con Dominios COBIT 2019

Cada dominio fue elegido considerando los valores asignados a factores de diseño como perfil de riesgo, cumplimiento, amenazas tecnológicas, tamaño de la organización y estrategia empresarial.

Esta alineación permite que la implementación del sistema de gobernanza sea personalizada y adecuada a las necesidades y capacidades del entorno institucional, el dominio APO12 (gestión de riesgos) responde directamente al nivel alto de exposición a amenazas y riesgos identificados, mientras que DSS05 (gestión de seguridad de servicios) atiende la necesidad urgente de controles de seguridad proactivos y monitoreo continuo.

Asimismo, la tabla XII muestra cómo los procesos APO01 y APO03 refuerzan el diseño y despliegue de políticas, marcos de referencia y arquitecturas tecnológicas coherentes.

Tabla XI.

RELACIÓN ENTRE VALOR DEL FACTOR DE DISEÑO Y ÁREAS PRIORITARIAS DE SEGURIDAD

Valor FD	Prioridad de los objetivos de gobierno y gestión	Componentes	Variantes del Área Prioritaria
Alto	Entre los objetivos de gobierno y gestión importantes se incluyen: ▪ APO01 – Gestionar el marco de gestión de TI ▪ APO03 – Gestionar la arquitectura empresarial ▪ APO12 – Gestionar el riesgo ▪ APO13 – Gestionar la seguridad ▪ DSS05 – Gestionar la seguridad de los servicios	Entre las estructuras organizativas importantes se encuentran: ▪ Comité de estrategia de seguridad ▪ Director de seguridad de la información Entre los aspectos de cultura y comportamiento organizacional se encuentran: ▪ Concienciación sobre seguridad Los flujos de información incluyen: ▪ Política de seguridad ▪ Estrategia de seguridad	Área prioritaria de seguridad de la información

Tabla XII.

RELACIÓN ENTRE FACTORES DE DISEÑO, DOMINIOS COBIT 2019 Y JUSTIFICACIÓN

Factor de Diseño	Dominio COBIT	Complemento / Justificación
Escenario de amenazas	APO12 – Gestionar el riesgo	Evalúa y gestiona el impacto de amenazas como ciberataques o pérdida de datos. Establece controles y medidas de mitigación.
Escenario de amenazas	APO13 – Gestionar la seguridad	Implementa políticas y procedimientos de seguridad de la información frente a amenazas externas e internas.

Cuadro XII– *continuación*

Factor de Diseño	**Dominio COBIT**	**Complemento / Justificación**
Escenario de amenazas	DSS05 – Gestionar la seguridad de los servicios	Asegura la continuidad de los servicios mediante controles preventivos, detección y respuesta a incidentes.
Estrategia empresarial	APO01 – Marco de gobernanza de TI	Alinea la TI con los objetivos estratégicos institucionales. Establece roles, políticas y principios de gobierno.
Estrategia empresarial	APO03 – Arquitectura empresarial	Permite planificar e integrar tecnología de forma estructurada en los procesos institucionales.
Perfil de riesgo	APO12 – Gestionar el riesgo	Identifica, clasifica y responde a los riesgos de TI. Genera planes de acción.
Perfil de riesgo	DSS05 – Seguridad de servicios	Implementa medidas de seguridad adaptadas al perfil de riesgo. Asegura los sistemas críticos.

Aplicar un factor de diseño implica analizar la situación actual de la organización en este caso, el GADP-Tufiño respecto a un aspecto clave, como la estrategia empresarial, los riesgos tecnológicos, el tamaño institucional, el objetivo de esta evaluación es identificar si dicho aspecto influye en la necesidad, prioridad o forma en que se deben implementar los procesos de gobernanza y gestión propuestos por COBIT 2019.

De esta manera, en la tabla XIII el uso de factores de diseño permite personalizar el sistema de gobernanza de TI, asegurando que los procesos seleccionados estén alineados con las condiciones reales y los objetivos estratégicos de la organización.

Tabla XIII.
EVALUACIÓN DE MADUREZ DE PROCESOS COBIT SEGÚN FACTORES DE DISEÑO

Proceso COBIT	**Factores de Diseño Evaluados**	**Promedio de Madurez**	**Observaciones**
APO001	DF1, DF2, DF7, DF11	0.67	Nivel inicial. Hay prácticas ejecutadas sin estructura ni documentación.
APO003	DF1, DF4, DF7	0.89	Nivel inicial. Hay prácticas ejecutadas sin estructura ni documentación.
APO012	DF2, DF3, DF5, DF6	0.44	Nivel muy bajo. No se evidencia una implementación formal ni controlada.
APO013	DF4, DF5, DF6	0.56	Nivel inicial. Hay prácticas ejecutadas sin estructura ni documentación.
DSS05	DF3, DF4, DF5, DF6	0.44	Nivel muy bajo. No se evidencia una implementación formal ni controlada.

Los resultados muestran que todos los procesos se encuentran en niveles de madurez entre 0.44 y 0.89, lo que indica que la organización apenas está iniciando la implementación de prácticas de gestión y gobierno de TI.

Para identificar el nivel de madurez utilizaremos el nivel objetivo sugerido de capacidad de procesos, tomando en cuenta que estamos trabajando con el modelo de capacidad de COBIT 2019, como se muestra en la tabla XIV.

Tabla XIV.
NIVELES DE MADUREZ Y OBJETIVOS SUGERIDOS POR PROCESO COBIT 2019

Proceso COBIT	Nivel de Madurez Promedio	Nivel Objetivo capacidad de procesos
APO001	0.67	2
APO003	0.89	1
APO012	0.44	2
APO013	0.56	4
DSS05	0.44	3

En la Fig. 26 podemos identificar el nivel de madurez actual con el nivel de madurez objetivo.

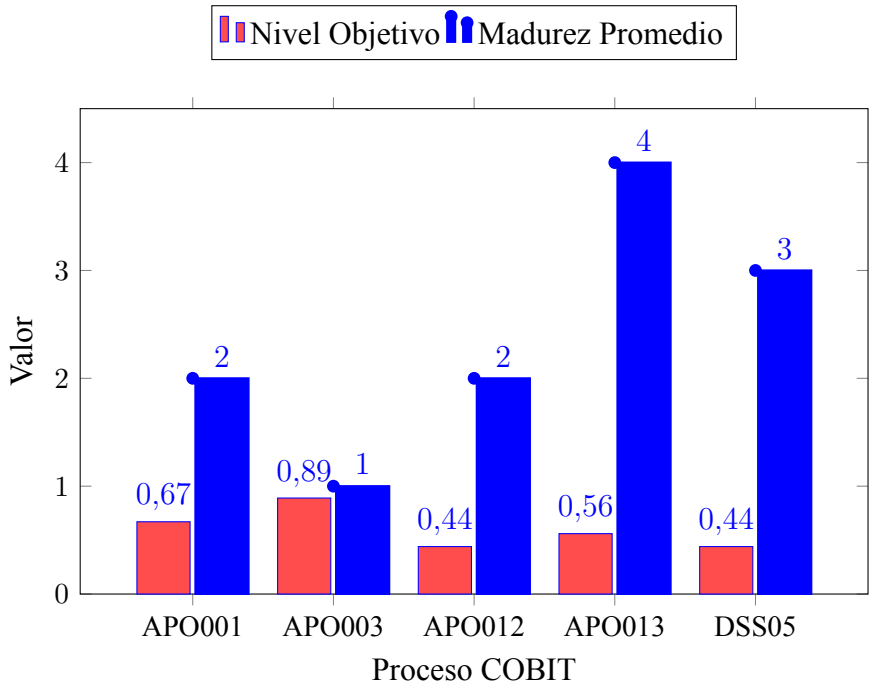


Fig. 26.. Brechas entre Nivel Actual vs Objetivo.

En la siguiente Tabla XV podemos observar las brechas, la madurez promedio y el nivel objetivo por proceso COBIT 2019.

Tabla XV.
ANÁLISIS DE MADUREZ, OBJETIVO Y BRECHA POR PROCESO COBIT 2019

Proceso COBIT	**Nivel de Madurez Promedio**	**Nivel objetivo sugerido de capacidad de procesos**	**Brecha**
APO001	0,67	2	1,33
APO003	0,89	1	0,11
APO012	0,44	2	1,56
APO013	0,56	4	3,44
DSS05	0,44	3	2,56

En la Fig. 27 se muestra el análisis de brechas, madurez promedio y nivel objetivo por proceso COBIT 2019.

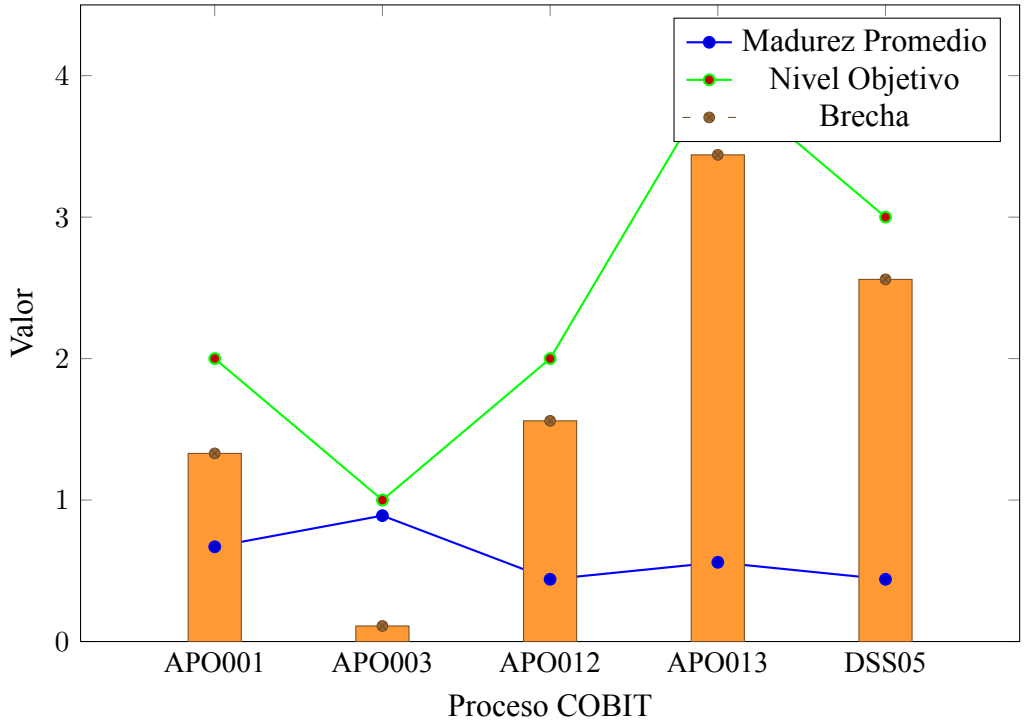


Fig. 27.. Brechas, madurez promedio y nivel objetivo por proceso COBIT 2019.

Media de Madurez Promedio

$$Madurez = \frac{\sum \text{madurez}}{n} \tag{3.1}$$

$$\frac{0{,}67 + 0{,}89 + 0{,}44 + 0{,}56 + 0{,}44}{5} = \frac{3}{5} = 0{,}6 \tag{3.2}$$

Este valor indica que, en promedio, los procesos evaluados se encuentran en un nivel de madurez muy básico, dado que el marco COBIT 2019 plantea niveles del 0 al 5, una media de 0.60 revela que la mayoría de los procesos están en fase de implementación inicial, sin prácticas estandarizadas ni controladas.

Implicación: Se requiere fortalecer la implementación de buenas prácticas y formalizar los procesos existentes.

Mediana de Madurez Promedio

Paso 1:

Ordenar los valores:

(0.44,0.44,0.56,0.67,0.89)

Paso 2:

Valor central (posición 3 de 5):

0.56

La mediana, cercana a la media, confirma que la distribución de la madurez es relativamente uniforme, sin presencia de valores extremos que distorsionen el promedio.

Esto refuerza el diagnóstico de que el bajo nivel de madurez es generalizado en todos los procesos analizados.

Desviación Estándar

La desviación estándar se calcula según la Ecuación (3.3):

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2} \tag{3.3}$$

Donde:

- $\bar{x} =$ media aritmética = 0.60
- $n =$ cantidad de valores = 5
- $x_i =$ cada valor individual

Cálculo:

$$(0{,}67 - 0{,}60)^2 = 0{,}0049$$

$$(0{,}89 - 0{,}60)^2 = 0{,}0841$$

$$(0{,}44 - 0{,}60)^2 = 0{,}0256$$

$$(0{,}56 - 0{,}60)^2 = 0{,}0016$$

$$(0{,}44 - 0{,}60)^2 = 0{,}0256$$

Promedio de cuadrados:

$$\frac{0{,}0049 + 0{,}0841 + 0{,}0256 + 0{,}0016 + 0{,}0256}{5} = 0{,}02836$$

Finalmente:

$$\sigma = \sqrt{0{,}02836} = \mathbf{0{,}188}$$

Una desviación estándar baja sugiere que los valores de madurez no varían demasiado entre procesos, lo cual es coherente con una organización que presenta una situación de madurez homogéneamente baja.

- Conclusión:

No hay procesos significativamente más avanzados que otros, lo que implica que las mejoras deben abordarse de manera integral.

Media de Nivel Objetivo

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

El nivel objetivo promedio representa el grado de madurez que se espera alcanzar según los requerimientos estratégicos del negocio.

Un valor de 2.4 indica que la organización aspira a que sus procesos estén definidos y gestionados, con roles claros, documentación y prácticas repetibles, la diferencia entre el valor actual (0.60) y el objetivo (2.4) muestra una brecha importante que requiere planificación y recursos.

En la tabla XVI se puede ver la **Media de Brecha (Nivel Objetivo - Madurez Promedio)**.

Tabla XVI.
CÁLCULO DE LA BRECHA POR PROCESO COBIT 2019

Proceso	**Brecha**
APO001	$2 - 0{,}67 = 1{,}33$
APO003	$1 - 0{,}89 = 0{,}11$
APO012	$2 - 0{,}44 = 1{,}56$
APO013	$4 - 0{,}56 = 3{,}44$
DSS05	$3 - 0{,}44 = 2{,}56$

$$\frac{1{,}33 + 0{,}11 + 1{,}56 + 3{,}44 + 2{,}56}{5} = \frac{9}{5} = 1{,}8$$

Este valor representa la distancia promedio entre el estado actual y el nivel deseado para cada proceso.

Una brecha de 1.8 puntos es significativa, y señala que la organización necesita escalar al menos dos niveles de madurez por proceso, lo cual no se logra sin una estrategia de gobernanza clara y sostenida.

3.8.1 Identificación de activos críticos de información

Esta herramienta permitió identificar las brechas en la infraestructura tecnológica, así como establecer un diagnóstico inicial del nivel de madurez en la implementación de controles de seguridad, clasificando los activos según su nivel de riesgo y criticidad para la organización.

PILAR aplica el enfoque de análisis de riesgos basado en la norma ISO/IEC 27002, que establece buenas prácticas para la gestión de la seguridad de la información, su uso puede complementarse de forma efectiva con el marco COBIT 2019, el cual permite evaluar y mejorar el nivel de madurez de los procesos tecnológicos mediante dominios y prácticas específicas.

Esta combinación facilita una evaluación integral que considera tanto la identificación de riesgos técnicos como la gobernanza y gestión de TI, proporcionando una visión clara del estado actual y las áreas prioritarias de mejora.

Además, al integrar la perspectiva de PILAR [42] con los factores de diseño de COBIT 2019, es posible personalizar las estrategias de gobernanza en función del contexto institucional, los objetivos estratégicos y las capacidades reales del GADP-Tufiño.

Esto permite no solo identificar los controles que requieren fortalecimiento, sino también priorizar acciones según la exposición al riesgo, el cumplimiento normativo y la criticidad de los servicios tecnológicos evaluados.

Interpretación General

Cada fila representa una salvaguarda (control de seguridad), evaluada en cuanto a su:

- Nivel actual (current) → qué tan implementada está.
- Nivel objetivo (target) → meta recomendada.
- Nivel de PILAR sugerido → en algunos casos aparece "L2-L5".

(desde nivel 2 hasta nivel 5 recomendado). tabla XVII

Tabla XVII.
EVALUACIÓN DE SALVAGUARDAS: SITUACIÓN ACTUAL Y NIVELES OBJETIVO

Aspecto	TDP	Recomendado	Salvaguarda	Current	Target
G	EL	8	Identificación y autenticación [IA]	-L1	L2-L5
T	EL	7	Control de acceso lógico [AC]	-L1	L2-L4
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	4	Protección de los Servicios	—	n.a.
G	PR	4	Protección de las Aplicaciones Informáticas (SW)	—	L2-L3
G	PR	4	Protección de los Equipos Informáticos (HW)	—	n.a.
G	PR	4	Protección de las Comunicaciones	—	L2-L3
G	PR	4	Protección de los Soportes de Información	—	L2-L3
G	PR	4	[AUX] Elementos Auxiliares	—	L2-L3
G	PR	5	[PE] Protección física de los equipos	L1	L3
G	PR	5	[P-I] Protección de las Instalaciones	-L1	n.a.
G	PR	5	[P] Gestión del Personal	-L1	n.a.
G	CR	5	[IM] Gestión de incidentes	-L1	L2-L3

Cuadro XVII– *continuación*

Aspecto	TDP	Recomendado	Salvaguarda	Current	Target
F	EL	8	[tools] Herramientas de seguridad	-L1	L2-L3
G	CR	5	[VR] Gestión de vulnerabilidades	—	L2-L3
G	CR	4	[A] Registro y auditoría	—	L2-L3
T	MN	4	[BG] Continuidad del negocio	—	L2-L3
G	RC	4	[E] Organización	—	L2-L3
G	AD	3	[NEW] Adquisición / desarrollo	-L1	L2-L3
G	AD	3	[PDS] Servicios potencialmente peligrosos	L0-L1	n.a.
G	PR	3	[IP] Sistema de protección de frontera lógica	—	n.a.
G	PR	3	[PPS] Protección del perímetro físico	-L1	L3
G	EL	3	[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]	-L1	n.a.

Significado de los niveles L0 a L5 de la aplicación PILAR, donde se realizó la evaluación de los activos críticos, tabla XVIII.

Tabla XVIII.

NIVELES DE MADUREZ E INTERPRETACIÓN PRÁCTICA

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 operando.
L4	Gestión activa	El control es monitoreado y revisado regularmente.
L5	Optimización y mejora continua	El control se mejora continuamente con métricas y análisis.

Podemos observar las salvaguardas, con avance parcial en la tabla XIX.

Tabla XIX.
SALVAGUARDAS AVANCE PARCIAL

Salvaguarda	Nivel Actual	Nivel Objetivo	Estado
Protección física de los equipos [PE]	L1	L2–L5	Inicial
Gestión del personal [P]	-L1	L2–L3	En desarrollo
Organización [O]	-L1	L2–L3	Débil

Salvaguardas No Prioritarias o "No Aplica" (n.a.) Algunas salvaguardas como:

- Protección de frontera lógica (IP)
- Protección del perímetro físico (PPS)
- TEMPSET

Se marcan como "n.a." → puede ser porque no están dentro del alcance del activo o aún no han sido evaluadas.

En la Fig. 28 se presentan las brechas, la madurez promedio y el nivel objetivo por proceso COBIT 2019.

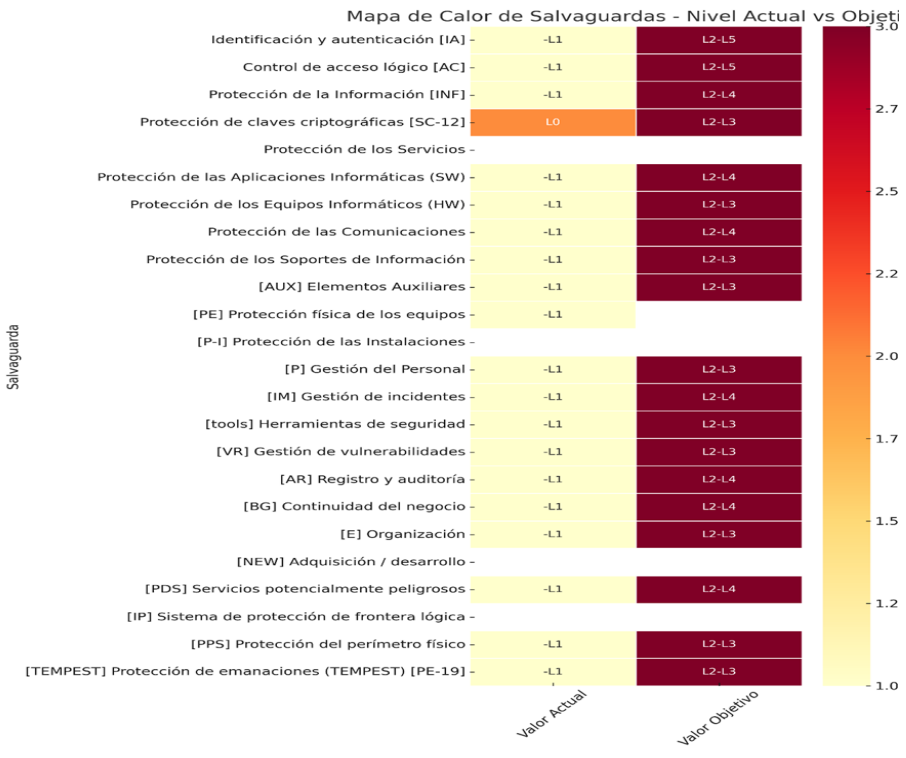


Fig. 28.. Mapa de Calor Salvaguardas.

INFORME DE ANÁLISIS DE SALVAGUARDAS - PILAR

Entidad Evaluada: GADP-Tufiño

Herramienta utilizada: PILAR

Fecha del Análisis: 24/03/2025

El presente análisis corresponde a la evaluación del nivel de implementación de las salvaguardas de seguridad de la información en la institución, de acuerdo con las recomendaciones generadas por la herramienta PILAR.

Cada control se ha comparado con su nivel actual y el nivel objetivo recomendado por la herramienta utilizada, se identifican brechas que requieren intervención inmediata para fortalecer la postura de seguridad institucional actual.

Salvaguardas Críticas con Nivel Bajo

Estas salvaguardas presentan nivel -L1 o L0, lo que indica un estado de no Implementación.

Con los resultados obtenidos en el nivel de salvaguardas se ha realizado el análisis de las brechas entre el nivel actual y el objetivo de las salvaguardas tabla XX.

Tabla XX.
SALVAGUARDAS CRÍTICAS CON NIVEL BAJO

Salvaguarda	**Nivel Actual**	**Nivel Objetivo**	**Comentario**
Identificación y autenticación [IA]	-L1	L2–L5	Alto riesgo
Control de acceso lógico [AC]	-L1	L2–L4	Sin controles sólidos
Protección de la Información [INF]	-L1	L2–L4	Alta exposición
Protección de claves criptográficas [SC-12]	L0	L2–L3	No hay control
Gestión de incidentes [IM]	-L1	L2–L3	Debilidad operativa
Gestión de vulnerabilidades [VR]	-L1	L2–L3	No hay proceso de gestión
Registro y auditoría [A]	-L1	L2–L3	Sin trazabilidad
Protección de las instalaciones [P-I]	-L1	L2–L3	Riesgo físico
Herramientas de seguridad [tools]	-L1	L2–L3	No se utilizan o configuran

En la Fig. 29 tenemos las brechas entre el nivel actual y el nivel objetivo.

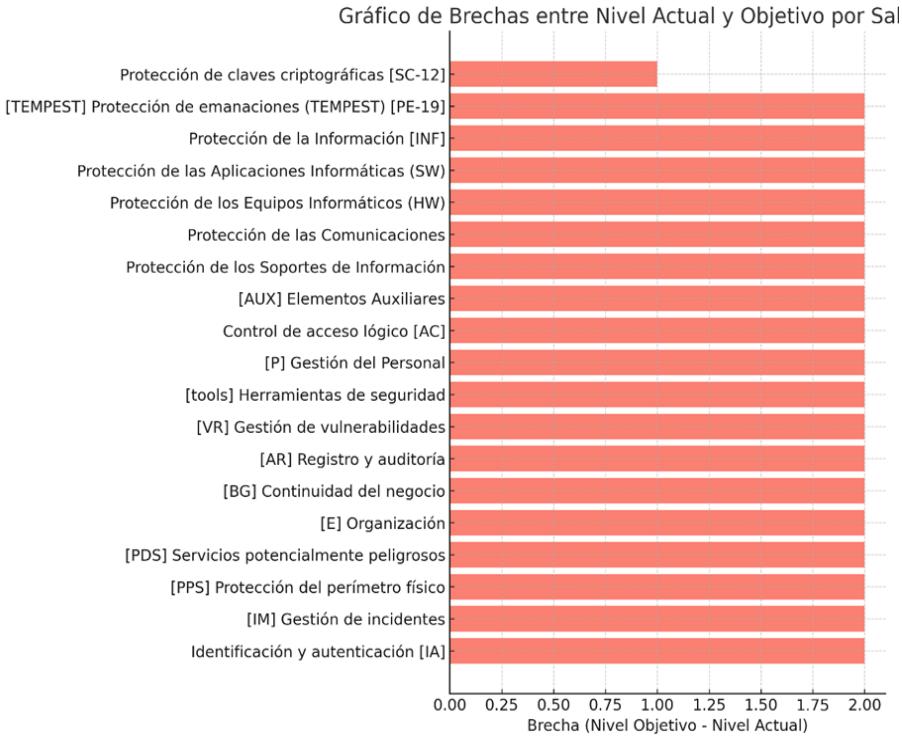


Fig. 29.. Brechas entre nivel actual y objetivo por salvaguardas. Autor propio.

3.8.2 Comparación con Nivel Deseado o Recomendado

Se estableció como referencia el Nivel 3 (Establecido), tanto en el modelo CMMI adaptado a COBIT 2019, como en el análisis de salvaguardas aplicado a través de PILAR, este nivel garantiza que los procesos están definidos, documentados y aplicados formalmente.

A continuación, se compararon los niveles actuales identificados para cada proceso y salvaguarda frente al nivel deseado (L3). Las diferencias detectadas reflejan brechas, las cuales indican debilidades de implementación o ausencia de controles, tabla XXI.

Tabla XXI.
BRECHAS DETECTADAS EN PROCESOS Y SALVAGUARDAS

Proceso / Salvaguarda	**Nivel Actual**	**Nivel Deseado**	**Brecha Detectada**
Identificación y autenticación [IA]	-L1	L3	Sí
Protección de la información [INF]	-L1	L3	Sí
Registro y auditoría [A]	-L1	L3	Sí
Gestión de riesgos (COBIT APO12)	0,6	≥3.0	Sí
Protección física de los equipos [PE]	L1	L3	Sí
Gestión de seguridad (COBIT APO13)	0,7	≥3.0	Sí

3.8.3 Identificar Debilidades En Los Controles De Seguridad

Al analizar el estado actual de los controles de seguridad en el GADP-Tufiño y detectar aquellas áreas en las que los mecanismos de protección son inexistentes, inadecuados o ineficaces, Con el fin de priorizar acciones correctivas alineadas a COBIT 2019, la Tabla XXII presenta las debilidades de control y riesgos asociados.

Tabla XXII.
DEBILIDADES DE CONTROL Y RIESGOS ASOCIADOS

Área de Control	**Debilidad Detectada**	**Riesgo Asociado**
Autenticación y acceso	No hay políticas de contraseñas ni doble factor	Suplantación de identidad, intrusiones
Protección de información	No hay respaldo ni cifrado de datos	Pérdida o fuga de información
Gestión de incidentes	No existe procedimiento ante incidentes	Tiempo de respuesta insuficiente
Seguridad perimetral	No se emplean herramientas de protección lógica	Acceso no autorizado
Registro y trazabilidad	No se realizan auditorías ni monitoreo de logs	Falta de evidencia ante anomalías

Existe una lista de debilidades comunes identificadas en los controles de seguridad, basada en tu evaluación con PILAR, encuestas y el marco de COBIT 2019 (especialmente dominios como APO13, DSS05, APO12):

A continuación, en la Tabla XXIII se redactan las acciones correctivas según COBIT 2019.

Tabla XXIII.
DEBILIDADES DETECTADAS Y ACCIONES DE MEJORA SUGERIDAS POR ÁREA DE CONTROL

Área de Control	**Debilidad Detectada**	**Acción de Mejora Sugerida**
Autenticación y acceso (IA)	No hay política de contraseñas ni doble factor de autenticación	Redactar política básica de contraseñas e implementar doble autenticación
Protección de la información (INF)	No existe respaldo cifrado ni política clara de almacenamiento seguro	Establecer copias de seguridad cifradas y reglas de almacenamiento seguro

Continúa en la siguiente página

Cuadro XXIII (continuación)

Área de Control	Debilidad Detectada	Acción de Mejora Sugerida
Gestión de incidentes (IM)	No hay protocolo ni responsable asignado para respuesta a incidentes	Asignar un encardo del GADP-Tufiño de seguridad y crear un protocolo de actuación
Registro y trazabilidad (A)	No se realizan auditorías, logs no revisados	Implementar revisión mensual de logs y definir un sistema de alertas
Seguridad perimetral (IP)	No se usan firewalls o antivirus corporativos configurados	Instalar firewall gratuito y antivirus actualizado en todos los equipos
Gestión de vulnerabilidades (VR)	No se identifican ni evalúan vulnerabilidades técnicas o humanas	Realizar escaneo periódico de vulnerabilidades y capacitar al personal

3.8.4 Aplicación de COBIT 2019 por Dominio

La aplicación del marco COBIT 2019, desglosado por dominios, permitió realizar un análisis profundo de la gobernanza de las tecnologías de la información dentro del GADP-Tufiño. Esta implementación facilitó la identificación de brechas de madurez al establecer una correlación directa entre los dominios del modelo y los controles existentes en los procesos tecnológicos.

A través de la evaluación de madurez de cada uno de estos dominios, fue posible detectar con mayor claridad las áreas débiles o vulnerables en la gestión de las tecnologías de información, tanto a nivel estratégico como operativo.

Los hallazgos obtenidos a partir de esta evaluación sirvieron como insumo clave para alimentar los planes de mejora continua, permitiendo priorizar proyectos enfocados en fortalecer la seguridad de la información, optimizar procesos tecnológicos.

APO01 – Gestión de Gobierno

- **Objetivo:** Asegurar que se establezca un marco de gobernanza claro que defina roles, políticas, normas y estructuras de decisión.
- **Cómo aplicarlo:** Desarrollar una política de seguridad de la información alineada con COBIT 2019.

APO03 – Gestión de la Arquitectura Empresarial

- **Objetivo:** Desarrollar y mantener una arquitectura que permita una integración eficiente entre los procesos del GADP-Tufiño y los sistemas de información.
- **Cómo aplicarlo:**
    a) Mapear los procesos clave del GADP-Tufiño (finanzas, servicios, seguridad) y su dependencia de TI.
    b) Alinear sistemas como PILAR, gestión documental y bases de datos con los objetivos institucionales.

APO12 – Gestión de Riesgos

- **Objetivo:** Identificar, evaluar y responder a riesgos relacionados con el uso de TI.
- **Cómo aplicarlo:**
    a) Utilizar los resultados de PILAR como base para el registro institucional de riesgos TI.
    b) Clasificar los riesgos por impacto (confidencialidad, disponibilidad, integridad).
    c) Establecer un plan de tratamiento de riesgos con responsables, tiempos e indicadores.

APO13 – Gestión de Seguridad

- **Objetivo:** Proteger la información y los activos de TI mediante políticas, controles y medidas adecuadas.
- **Cómo aplicarlo:** Diseñar e implementar políticas de seguridad como control de accesos y gestión de contraseñas.

DSS05 – Gestión de Servicios de Seguridad

- **Objetivo:** Garantizar que los servicios de seguridad operen de manera eficiente y respondan adecuadamente ante incidentes.
- **Cómo aplicarlo:**

a) Implementar un procedimiento de gestión de incidentes que contemple el reporte, análisis y resolución.

b) Emplear herramientas de monitoreo (antivirus, firewalls, sistemas de alertas) de acuerdo con las recomendaciones de PILAR.

3.8.5 Práctica con el diagnóstico

Se presenta un resumen ejecutivo de los hallazgos y recomendaciones basados en el marco COBIT 2019 y los resultados del análisis de seguridad PILAR, se abordan cinco dominios clave, identificando brechas y proponiendo acciones correctivas específicas.

En la Tabla XXIV podemos ver el detalle de la práctica bajo el diagnóstico obtenido.

Tabla XXIV.
MATRIZ DE APLICACIÓN DE COBIT 2019 EN EL GADP-TUFIÑO

Dominio COBIT	**Objetivo Principal**	**Relación con Análisis PILAR**	**Acciones Recomendadas**	**Evidencia Esperada**
APO01 Marco de Gobierno	Establecer estructura de gobernanza para TI	No existe una estructura formal de gobernanza	Aprobar una política de seguridad de la información alineada con COBIT 2019	Políticas institucionales
APO03 Arquitectura Empresarial	Integrar procesos institucionales con TI	Los activos críticos no están alineados a procesos claves	Mapear procesos, definir estándares	Mapa de procesos, arquitectura de sistemas, catálogo de aplicaciones
APO12				

Continúa en la siguiente página

Cuadro XXIV (continuación)

Dominio COBIT	**Objetivo Principal**	**Relación con Análisis PILAR**	**Acciones Recomendadas**	**Evidencia Esperada**
Gestión de Riesgos	Identificar y tratar riesgos de TI	PILAR identifica riesgos críticos en confidencialidad, disponibilidad y autenticidad	Crear registro de riesgos, establecer responsables y medidas de mitigación	Registro de riesgos, plan de tratamiento, cronograma de mitigación
APO13 Gestión de Seguridad	Proteger información institucional	Múltiples salvaguardas están en nivel -L1 o L0	Diseñar e implementar políticas de seguridad, fortalecer controles	Políticas firmadas, controles implementados, reportes de cumplimiento
DSS05 Gestión de Servicios de Seguridad	Operar servicios de seguridad y responder incidentes	No existen procedimientos formales de incidentes	Definir procedimiento de incidentes	Procedimiento escrito, registro de incidentes

3.8.6 Comparación del Estado Actual vs. Mejores Prácticas - COBIT 2019

Entidad: GADP-Tufiño

Objetivo: Determinar la brecha entre el nivel actual de madurez de los dominios COBIT 2019, los dominios seleccionados y las mejores prácticas de referencia se presentan en la Tabla XXV.

Tabla XXV.

EVALUACIÓN DE DOMINIOS COBIT 2019 EN EL GADP-TUFIÑO

Dominio COBIT	Descripción del Dominio	Estado Actual	Nivel Ideal	Brecha	Observaciones
APO01 - Marco de Gobierno	Estructura de gobernanza de TI, políticas institucionales	Nivel 1 - Realizado parcialmente, sin políticas vigentes	Nivel 3 - Gobernanza establecida, con políticas institucionales	Alta	Requiere formalizar estructura y aprobar normativas.
APO03 - Arquitectura Empresarial	APO01 de procesos institucionales y sistemas de información	Nivel 1 - No existe documentación formal de procesos ni arquitectura definida	Nivel 3 - Arquitectura documentada y alineada a necesidades institucionales	Alta	Debe mapearse la infraestructura TI y los procesos clave.
APO12 - Gestión de Riesgos	Identificación, evaluación y tratamiento de riesgos de TI	Nivel 2 - Diagnóstico con PILAR realizado, pero sin gestión formal continua	Nivel 4 - Gestión de riesgos predecible, con responsables, controles y planes	Media-Alta	Se debe implementar seguimiento, revisiones y actualización de riesgos.
APO13 - Seguridad de la Información	Protección de la información y los activos mediante políticas y controles	Nivel 1 - Políticas en construcción, controles parcialmente implementados	Nivel 3 - Seguridad institucionalizada, con controles activos y revisiones periódicas	Alta	Priorizar salvaguardas críticas como IA, AC, INF.
DSS05 - Servicios de Seguridad	Operación de servicios de seguridad y gestión de incidentes	Nivel 1 - No existe procedimiento formal ni trazabilidad de incidentes	Nivel 3 - Procedimientos operativos establecidos, indicadores y registros	Muy Alta	Implementar plan de respuesta a incidentes y registros de eventos.

3.9 Identificación de Brechas

La identificación de brechas en seguridad de la información y gobernanza de TI se realizó a través de un enfoque combinado que permitió evaluar tanto el estado técnico como organizacional del GADP-Tufiño:

a) Se utilizó la herramienta PILAR (Politically Independent Layered Architecture for Risk Analysis), que permite analizar el grado de implementación de las salvaguardas de seguridad basadas en la norma ISO/IEC 27002. Este análisis permitió:

   - Establecer los niveles actuales de implementación.
   - Determinar el nivel objetivo deseado para cada salvaguarda.
   - Detectar riesgos y clasificar la criticidad de los activos tecnológicos.

b) Evaluación de Madurez usando Diseño de Factores con el modelo de capcidad de COBIT 2019 GADP-Tufiño:

Se empleó el modelo de capacidades (niveles 0 a 5), adaptado al marco de COBIT 2019, evaluando los siguientes dominios clave:

- APO01 – Gestión de gobernanza
- APO03 – Gestión de la arquitectura empresarial
- APO12 – Gestión de riesgos
- APO13 – Gestión de seguridad
- DSS05 – Gestión de servicios de seguridad

La madurez fue medida a través de encuestas dirigidas a los principales responsables institucionales (Presidente, Secretario y Responsable de TI), cuyas respuestas se convirtieron en puntuaciones numéricas de 0 a 5 para su análisis comparativo.

3.10 Evaluar Riesgos Asociados a las Brechas Encontradas

Este informe tuvo como objetivo evaluar los riesgos vinculados a las brechas detectadas en los controles de seguridad y su nivel de madurez, así como correlacionar estos hallazgos con un escaneo técnico realizado mediante la herramienta Nmap sobre la IP190.63.112.92. La combinación de ambos análisis (administrativo y técnico) permite obtener una visión integral del estado de seguridad de la organización, abordando tanto la configuración de políticas internas como la

exposición real en la red. Relación con Evaluación de Madurez El análisis de madurez identificó varios controles con una brecha significativa entre el estado actual y el objetivo deseado, particularmente en áreas como:

- Política de seguridad de la información
- Clasificación de la información
- Autenticación de usuarios
- Gestión de activos

Estos controles, si bien no muestran una exposición directa en el escaneo externo (sin puertos abiertos), representan riesgos internos o latentes que podrían materializarse si el entorno cambia o si se relajan las políticas actuales. Imagen del Sofware Informe de Análisis de Escaneo Nmap Dirección IP escaneada: 190.63.112.92 Host: customer-190-63-112-92.claro.com.ec Fecha del escaneo: 07 de marzo de 2025 Duración total: 6 horas y 9 minutos (22145.52 segundos) Herramienta utilizada: Nmap 7.95 Tipo de escaneo: Ping Scan, DNS, SYN Stealth Scan, OS Detection, Traceroute, NSE Scripts

a) **Estado General**

   - El host está activo (respuesta positiva al Ping).
   - Tiempo de respuesta promedio (latencia): 0.35 segundos.
   - Estado de los Puertos
   - Se escanearon 1000 puertos TCP estándar.
   - 919 puertos filtrados (no respondieron).
   - 81 puertos cerrados (responden pero sin servicio).
   - 0 puertos abiertos fueron detectados. Esto indica que el sistema está bien protegido a nivel de red, posiblemente por firewalls que filtran todo el tráfico entrante.

b) **Detección del Sistema Operativo (OS)**

   Aunque no se encontraron puertos abiertos que permitan una detección precisa, se obtuvieron estas posibles coincidencias del sistema operativo.

c) **Ruta de Red (Traceroute)**

   - Puerto utilizado: 3389/tcp (Remote Desktop Protocol).

- El traceroute mostró 30 saltos, lo cual es esperado para redes públicas y conexiones de larga distancia.
- Los detalles intermedios fueron omitidos por Nmap, probablemente por filtros ICMP o NAT.

d) **Observaciones de Seguridad**

- El nivel de exposición es bajo debido a que no hay puertos abiertos expuestos al escaneo.
- La presencia de puertos filtrados sugiere el uso de firewall o políticas de acceso restrictivas.
- No se detectaron servicios activos públicamente, lo cual es positivo desde una perspectiva defensiva.

3.11 Fase 2: Propuesta de Mejoras

La propuesta de mejora esta diseñada en la aplicación del Marco COBIT 2019, se han priorizado dominios para el mejor desarrollo en el marco de la seguridad TI, como son los dominios APO01, APO03, APO12, APO13, DSS05.

Esta propuesta surge del análisis conjunto de tres fuentes clave: Evaluación de Salvaguardas mediante la herramienta PILAR, que reveló brechas significativas en controles como autenticación, clasificación de la información y gestión de activos.

Escaneo de Vulnerabilidades Externas (Nmap), el cual mostró una superficie de ataque baja, pero también una limitada visibilidad de sistemas y servicios, lo que sugiere una necesidad de fortalecer la gestión y monitoreo interno.

La encuesta, identificó un bajo nivel de implementación en políticas de seguridad, roles y responsabilidades, así como falta de trazabilidad y mejora continua.

3.11.1 APO01 – Gestión de Gobernanza

Debilidad Detectada: No existe una estructura formal para la toma de decisiones tecnológicas.

Política Sugerida

1. Uso de contraseñas y actualizaciones periódicas.
2. Prohibición al compartir cuentas y contraseñas.
3. Instalación de software no autorizado.

4. Uso restringido de dispositivos USB personales.
5. Almacenamiento y respaldo de archivos de trabajo.
6. Uso de internet con fines laborales.
7. Reporte de anomalías y fallas informáticas.
8. Política de Gobernanza y Roles de TI.
9. Política de Uso Aceptable y Responsabilidades del Usuario Final.

Acción de Mejora

- Definir una política de contraseñas que establezca un mínimo de ocho caracteres y su renovación cada tres meses.
- Implementar controles técnicos que obliguen al cambio de contraseña en el período establecido.
- Comunicar y capacitar al personal sobre la importancia de mantener la confidencialidad de las contraseñas.
- Establecer políticas de uso individual de cuentas y prohibir expresamente el intercambio de credenciales.
- Monitorear accesos para detectar posibles usos compartidos.
- Aplicar sanciones en caso de incumplimiento.
- Implementar una política de gestión de software que prohíba instalaciones no autorizadas.
- Utilizar herramientas de gestión de activos para monitorear y controlar el software instalado.
- Realizar auditorías periódicas para asegurar el cumplimiento.
- Establecer una política de uso de dispositivos USB que requiera autorización previa.
- Configurar sistemas para bloquear dispositivos no autorizados.
- Capacitar al personal sobre los riesgos asociados al uso de dispositivos externos.
- Designar carpetas institucionales para el almacenamiento de archivos.

- Implementar políticas de respaldo que aseguren copias semanales de la información.
- Monitorear y verificar la realización de los respaldos.
- Establecer una política de uso aceptable de internet que priorice actividades laborales.
- Monitorear el uso de internet para detectar actividades no relacionadas con el trabajo.
- Educar al personal sobre el uso responsable de los recursos tecnológicos.
- Implementar un procedimiento de reporte de incidentes que permita a los usuarios informar problemas de manera eficiente.
- Asignar responsabilidades claras al responsable TIC para la gestión de incidentes.
- Capacitar al personal sobre la importancia de reportar anomalías oportunamente.
- Supervisar el cumplimiento de las políticas de seguridad TIC.
- Ejecutar y verificar respaldos periódicos de la información institucional.
- Coordinar la instalación y actualización de antivirus y cortafuegos.
- Capacitar al personal en buenas prácticas de seguridad informática.
- Acatar las normas establecidas en la política de seguridad.
- Utilizar responsablemente los equipos tecnológicos y la información institucional.
- Reportar inmediatamente cualquier incidente relacionado con la seguridad o uso indebido de tecnologías.

Resultado Esperado: Se espera que la organización cuente con un marco formal de gobernanza de TI que defina claramente los roles, responsabilidades y políticas, fortaleciendo la toma de decisiones tecnológicas, aumentando la seguridad y disponibilidad de la información institucional, y promoviendo una cultura organizacional donde el personal asuma activamente su rol en la protección y uso adecuado de los recursos tecnológicos.

3.11.2 APO03 – Gestión de la Arquitectura

Debilidad Detectada: No se tiene claro qué sistemas o equipos se usan para qué procesos.

Política Sugerida

1. Diseño de procesos centrados en el usuario.
2. Documentación y mantenimiento del mapa de procesos.
3. Gestión de tecnologías alineadas a los procesos.
4. Atención ciudadana multicanal y eficiente.
5. Mejora continua e innovación.

Acciones de Mejora

- Todos los procesos institucionales deben ser diseñados o rediseñados considerando su impacto en el servicio al ciudadano.
- Se priorizará la simplificación, estandarización y automatización de trámites.
- Se debe mantener actualizado un mapa de procesos institucionales, clasificados por tipo (estratégicos, misionales, de apoyo).
- Toda área del GADP-Tufiño es responsable de documentar y revisar sus procesos al menos una vez al año.
- Toda adquisición o implementación tecnológica debe responder a una necesidad procesal identificada y justificada.
- Las tecnologías deben estar integradas para permitir la trazabilidad de la información y reducir duplicidades.
- Se fomentará el uso de tecnologías digitales para la atención al ciudadano: portales web, aplicaciones móviles, sistemas de seguimiento en línea, etc.
- Se garantizará que los canales digitales sean accesibles, confiables y fáciles de usar.
- Los procesos deben ser revisados periódicamente para identificar oportunidades de mejora, apoyados por datos y retroalimentación del usuario.
- Se promoverá una cultura de innovación en la gestión pública local.

Resultado Esperado: Se espera que el GADP-Tufiño cuente con una arquitectura empresarial bien definida, con procesos institucionales documentados, estandarizados y apoyados por tecnologías alineadas estratégicamente, lo que permitirá una atención al ciudadano más ágil, eficiente y transparente, fortaleciendo la gobernanza, optimizando recursos y promoviendo una cultura de mejora continua en la gestión pública.

3.11.3 APO12 – Gestión de Riesgo

Debilidad Detectada: No hay gestión activa de riesgos informáticos.

Política Sugerida

1. Identificación sistemática de riesgos de TI.
2. Registro y evaluación de riesgos.
3. Acciones de mitigación y responsables.
4. Sensibilización y capacitación.

Acciones de Mejora

- Se deben identificar de forma proactiva los riesgos que puedan afectar la infraestructura tecnológica, los sistemas de información, la ciberseguridad y la continuidad de los servicios.
- Todos los riesgos identificados deberán ser registrados en una matriz institucional, indicando sus causas, probabilidad, impacto y nivel de riesgo.
- Se deben priorizar los riesgos que representen una amenaza significativa para la operación y los servicios críticos del GADP-Tufiño.
- Para cada riesgo identificado, se deben establecer acciones de mitigación y asignar responsables claros para su tratamiento.
- Se promoverá la integración del análisis de riesgos en la toma de decisiones y planificación de proyectos tecnológicos.
- La matriz de riesgos deberá actualizarse al menos cada seis meses o cuando se presenten cambios significativos en el entorno tecnológico.
- El personal deberá recibir capacitación básica sobre gestión de riesgos tecnológicos y su rol en la prevención de incidentes.

Resultado Esperado: Los riesgos y causas identificadas se presentan en la Tabla XXVI, donde el GADP-Tufiño, contará con una gestión activa y documentada de los riesgos informáticos, lo que permitirá anticiparse a eventos adversos, reducir vulnerabilidades tecnológicas, proteger la información institucional y fortalecer la resiliencia operativa ante incidentes.

Tabla XXVI.
MATRIZ DE RIESGOS PARA EL PROCESO APO012

Riesgo	Causa Identificada	Prob. (1-5)	Impacto (1-5)	Nivel de Riesgo
Pérdida o filtración de información sensible	Falta de controles de acceso y políticas de cifrado	4	5	Alto
Interrupción de servicios críticos de TI	Ausencia de planes de continuidad y respaldo	3	5	Medio-Alto
Acceso no autorizado a sistemas	Uso de contraseñas débi-les, sin autenticación	4	4	Alto
Retrasos en la respuesta a incidentes	Falta de procedimientos y personal asignado	3	4	Medio-Alto
Riesgos legales por in-cumplimiento normativo	Falta de conocimiento o actualización de normas	2	5	Medio-Alto

3.11.4 APO13 – Gestión de Seguridad

Debilidad Detectada: Faltan políticas básicas de seguridad y protección de datos.

Política Sugerida:

1. Buenas prácticas para contraseñas y uso de dispositivos.
2. Uso responsable de equipos y dispositivos.
3. Uso del correo electrónico y navegación.
4. Guardar archivos en lugares seguros.
5. Proteger el acceso a los archivos.
6. Evitar riesgos comunes.
7. Realizar respaldos periódicos.

Acciones de Mejora:

- Las contraseñas deben tener una longitud mínima de ocho (8) caracteres.
- Se recomienda una combinación de letras mayúsculas, minúsculas, números y símbolos especiales.

- No deben incluir datos personales ni secuencias comunes como “123456” o palabras como “admin”.
- Está prohibido compartir contraseñas con otras personas, incluso con personal técnico.
- Las contraseñas deberán actualizarse al menos cada tres (3) meses.
- Solo se permite la instalación de software autorizado por el responsable TIC.
- No conectar dispositivos USB personales sin aprobación previa.
- El antivirus debe mantenerse actualizado y no deben descargarse archivos de fuentes no confiables.
- Al dejar el equipo sin supervisión, debe cerrarse la sesión o bloquearse el acceso.
- Cada usuario debe realizar copias de seguridad semanales de su información laboral.
- No abrir correos sospechosos ni con remitentes desconocidos.
- Evitar hacer clic en enlaces o archivos adjuntos no solicitados o sospechosos.
- El correo institucional debe usarse exclusivamente para fines laborales.
- No acceder a sitios web ajenos a las funciones del GADP-Tufiño desde equipos institucionales.
- Usar únicamente carpetas designadas como “Documentos GADP-Tufiño”, “Contabilidad” o “Informes”.
- Preferir el almacenamiento en unidades de red compartidas para documentos importantes.
- Evitar guardar archivos en el escritorio o la carpeta de descargas.
- Utilizar contraseñas de acceso en documentos mediante funciones de protección de software.
- Almacenar información en carpetas restringidas o dispositivos con cifrado.
- No enviar archivos sensibles mediante redes sociales, apps de mensajería o correos personales.

- Está prohibido conectar memorias USB desconocidas.
- No guardar contraseñas ni documentos delicados en papel o notas sueltas.

Resultado Esperado: La institución contará con políticas básicas de seguridad de la información y protección de datos formalmente definidas, comunicadas y aplicadas, lo que permitirá reducir vulnerabilidades, prevenir accesos no autorizados y promover una cultura de uso seguro y responsable de los recursos tecnológicos por parte del personal del GADP-Tufiño.

3.11.5 DSS05 – Gestión de Servicios de Seguridad

Debilidad Detectada: No hay un plan claro para actuar ante incidentes.

Política Sugerida

1. Ataque informático detectado (virus, phishing, acceso no autorizado).
2. Caída del sistema o de algún programa.
3. Pérdida de datos o archivos importantes.

Acciones de Mejora

- No apagar el equipo afectado.
- Desconectar el equipo de la red (desactivar conexión Wi-Fi o retirar el cable de red).
- Anotar los detalles observados (mensajes extraños, comportamiento anormal, ventanas emergentes, etc.).
- Comunicar el incidente de inmediato al responsable TIC.
- No reiniciar el equipo repetidamente.
- Esperar al menos dos minutos y documentar el mensaje de error que se presenta.
- Verificar si otros usuarios presentan el mismo inconveniente.
- Informar el incidente al responsable TIC para su análisis y resolución.
- Revisar si el archivo se encuentra en la papelera de reciclaje o si existe una copia en los respaldos locales.
- No utilizar programas externos para intentar recuperar los datos sin autorización técnica.
- Registrar y comunicar la información relevante al responsable TIC.

Resultado Esperado Mejor capacidad de respuesta ante amenazas. Las mejoras propuestas han sido simplificadas para facilitar su aplicación inmediata por parte del GADP-Tufiño, sin requerir grandes recursos técnicos.

3.11.6 Evaluación del plan de mejoras

Con base en los resultados del diagnóstico y el análisis obtenidos de las brechas identificadas, se planteó el plan de mejora orientado a fortalecer la seguridad institucional, esta propuesta contempló tanto los controles técnicos como medidas administrativas, incluyeron el desarrollo y formalización de políticas de seguridad en torno al marco COBIT 2019, la implementación de campañas internas de sensibilización y la incorporación de mecanismos de seguimiento y auditoría para asegurar la continuidad de la organización.

Para validar si es pertinente y la eficacia del plan, se aplicó la metodología Delphi, utilizada para alcanzar consensos entre expertos y verificar su alineación con los dominios del marco COBIT 2019, esta herramienta empleada en cada uno de los dominios ayudo a la toma de decisiones estratégicas, como también permitió evaluar la capacidad de la organización para responder ante amenazas y mejorar la resiliencia tecnológica.

La evaluación contó con la participación de diez especialistas en ciberseguridad y gobernanza de tecnologías de la información, pertenecientes a los sectores público y privado, el proceso se estructuró en dos rondas de cuestionarios anónimos, cada una seguida de retroalimentación, hasta lograr un alto nivel de acuerdo entre los participantes.

En la primera etapa, los expertos calificaron los dominios APO01, APO03, APO12, APO13 y DSS05 mediante una matriz de madurez con una escala de 0 a 5 y un esquema Likert de cinco puntos. Entre las recomendaciones surgidas destacó la incorporación del dominio MEA01 para reforzar la auditoría interna y la mejora continua, unificar algunas normas y correctamente cada una de las normas a los dominios utilizados, con énfasis en la documentación, evaluación y monitoreo de controles, así como en el fortalecimiento de políticas específicas relacionadas con respaldo de información, los roles de gobernanza y gestión de incidentes. Este ejercicio permitió no solo evidenciar debilidades en las áreas de gobernanza, gestión de riesgos, seguridad informática y servicios, sino también definir un conjunto de acciones concretas para elevar la madurez institucional y garantizar la protección de la información crítica en un entorno cada vez más expuesto a riesgos tecnológicos.

En la Fig. 30 se presentan las medias y desviaciones estándar de las evaluaciones por dominio,

lo que permite identificar claramente aquellas políticas con bajo desempeño promedio y alta variabilidad entre evaluadores, indicando posibles inconsistencias o criterios poco claros. A partir de estos hallazgos se realizaron ajustes y clarificaciones en las políticas evaluadas.

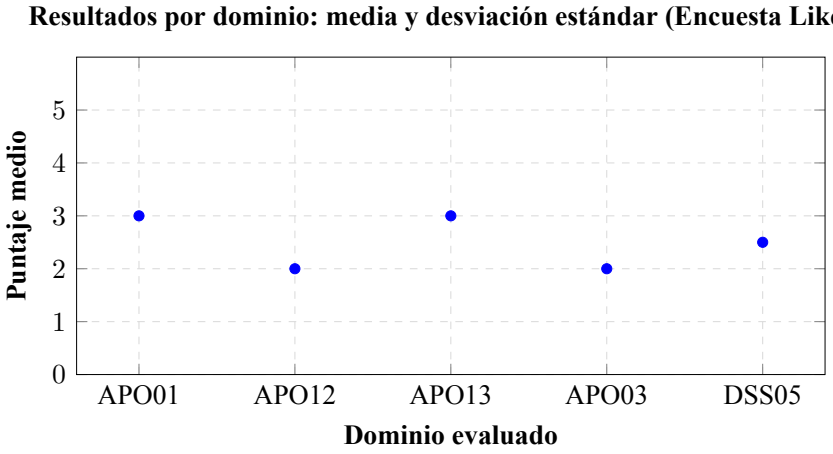


Fig. 30. Media y desviación estándar de aceptación por dominio en encuesta tipo Likert.

La Tabla XXVII evidencia que el entorno evaluado presenta una implementación sólida y madura de los procesos de gobernanza y gestión de TI, sin que se identifiquen debilidades relevantes, manteniéndose dentro de niveles aceptables. Destacan los dominios DSS05 y APO12 por su desempeño optimizado, mientras que APO01, APO03 y APO013 requieren intervenciones puntuales para elevar sus prácticas al siguiente nivel. En general, estos hallazgos confirman que el entorno de TI está bien gestionado y seguro, cumpliendo con las mejores prácticas internacionales.

Tabla XXVII.
MADUREZ PROMEDIO POR DOMINIO

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

Despues de haber aplicado los cambios sugeridos por los expertos en la primera ronda se aplico una segunda ronda de avaluación, El Índice de Aceptación se calculó a partir del promedio general obtenido (4,60 4,60), utilizando la expresión mostrada en la Ecuación 3.4:

$$\text{Índice de Aceptación} = \frac{4{,}60}{5} \cdot 100 = 92 \tag{3.4}$$

Este resultado refleja el porcentaje de aceptación con respecto al valor máximo posible en la escala utilizada. El índice global alcanzó un 92 %, lo que evidencia un nivel favorable dentro de la escala máxima de 5 puntos. Esto sugiere que, en términos generales, la percepción sobre el cumplimiento y la madurez de los dominios evaluados se encuentra en el nivel optimizado, en la segunda ronda, después aplicar el instrumento con las correcciones realizadas de la primera evaluación, no se identificaron nuevas observaciones ni variaciones significativas en las puntuaciones, confirmando así el nivel de madurez previsto y una validación metodológica satisfactoria.

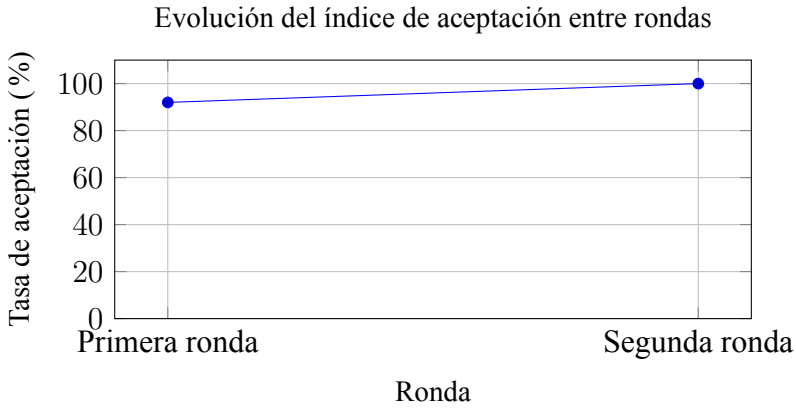


Fig. 31. Evolución de la tasa de aceptación entre la primera y segunda ronda de evaluación.

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, con estos resultados obtenidos de la segunda ronda, las políticas de seguridad realizas quedaron de la siguiente manera:

APO01 – Gestión de Gobernanza

Debilidad Detectada: Limitada estructura organizacional tecnológica para tomar decisiones de gestión y gobierno de TI.

Política Sugerida

1. Instalación de software no autorizado.
2. Uso restringido de dispositivos USB personales.
3. Almacenamiento y respaldo de archivos de trabajo.
4. Uso de internet con fines laborales.
5. Reporte de anomalías y fallas informáticas.

6. Política de Gobernanza y Roles de TI.

7. Definición de roles, responsable TI y estructura de gobernanza

APO03 – Gestión de la Arquitectura

Debilidad Detectada: Ausencia de un inventario estructurado y de una matriz de relacionamiento entre activos tecnológicos (sistemas, equipos, aplicaciones) y los procesos institucionales que respaldan

Política Sugerida

1. Diseño de procesos centrados en el usuario.

2. Documentación y mantenimiento del mapa de procesos.

3. Gestión de tecnologías alineadas a los procesos.

4. Atención ciudadana multicanal y eficiente.

APO12 – Gestión de Riesgo

Debilidad Detectada: No hay gestión activa de riesgos informáticos.

Política Sugerida

1. Identificación sistemática de riesgos de TI.

2. Registro y evaluación de riesgos.

3. Acciones de mitigación y responsables.

APO13 – Gestión de Seguridad

Debilidad Detectada: Ausencia de políticas institucionales formales y aprobadas que regulen los aspectos fundamentales de seguridad de la información y protección de datos.

Política Sugerida:

1. Uso responsable de equipos y dispositivos.

2. Uso del correo electrónico y navegación.

3. Evitar riesgos comunes.

4. Realizar respaldos periódicos.

5. Política de Uso Aceptable y Responsabilidades del Usuario Final.

6. Sensibilización y capacitación.

DSS05 – Gestión de Servicios de Seguridad

Debilidad Detectada: No hay un plan claro para actuar ante incidentes.

Política Sugerida

1. Ataque informático detectado (virus, phishing, acceso no autorizado).
2. Caída del sistema o de algún programa.
3. Las credenciales deberán cumplir con los estándares institucionales de seguridad, renovarse periódicamente y mantenerse de forma individual. Se prohíbe el uso compartido de cuentas.
4. Los archivos deben almacenarse en ubicaciones seguras y con accesos controlados, garantizando protección, trazabilidad y disponibilidad conforme a la política de seguridad de la organización.
5. Pérdida de Datos o Archivos Importantes

Esto demuestra que COBIT 2019 no se limita únicamente al entorno empresarial, ya que también abarca aspectos clave como el análisis del manejo de la información, la protección de los datos, la asignación clara de responsabilidades y la gestión institucional de las tecnologías de la información, la combinación de COBIT 2019 con la metodología Delphi se consolida como una estrategia eficaz y adaptable para fortalecer la gobernanza de TI, incluso en organizaciones con recursos limitados o con estructuras organizativas complejas.

La evaluación planteada en dos rondas, permitió alcanzar consensos entre expertos, priorizar acciones de mejora y alinear los procesos tecnológicos con las mejores prácticas internacionales, contribuyendo así a una gestión, eficiente y orientada a la toma de decisiones estratégicas.

3.12 Fase 3: Capacitación y Sensibilización

Jornadas de formación sobre buenas prácticas en seguridad informática, capacitar al personal administrativo y técnico en el uso seguro de tecnologías, prevención de riesgos digitales y cumplimiento de políticas de seguridad, con un enfoque práctico y accesible, la estructuración de jornadas se detalla en la Tabla XXVIII.

Tabla XXVIII.
ESTRUCTURACIÓN DE JORNADAS DE CAPACITACIÓN

Módulo	Tema	Duración	Modalidad
1	Introducción a la seguridad informática	15 min	Exposición
2	Errores comunes en el trabajo diario	15 min	Casos reales
3	Buenas prácticas con contraseñas	15 min	Demostración
4	Uso seguro del correo y navegación web	20 min	Vídeo práctico
5	Protección de archivos sensibles	20 min	Actividad guiada
6	Actuación ante incidentes informáticos	20 min	Simulación

Materiales de Apoyo

- Guía detallada con las principales reglas de seguridad TIC.
- Instructivo rápido de acciones a seguir ante incidentes informáticos.
- Ejemplos visuales de correos electrónicos falsos (phishing) y contraseñas vulnerables.
- Formulario físico de registro de asistencia.
- Evaluación digital mediante formulario en línea.

Resultados Esperados

- Incremento de la conciencia del personal sobre su rol en la protección de la información institucional.
- Reducción de incidentes causados por errores humanos, como ataques de phishing o pérdida de datos.
- Cumplimiento más riguroso de las políticas internas de seguridad de la información.
- Mejora en el nivel de madurez del dominio DSS05, conforme al marco de referencia COBIT 2019.

3.12.1 Difusión de políticas de seguridad adoptadas

Mediante esta aplicación nos aseguramos que todo el personal conozca, comprenda y aplique las políticas de seguridad institucional, promoviendo una cultura de protección de la información y uso responsable de los recursos tecnológicos, los medios y acciones se detallan en la Tabla XXIX.

Tabla XXIX.
MEDIOS DE DIFUSIÓN Y ACCIONES ESPECÍFICAS PARA COMUNICAR POLÍTICAS DE SEGURIDAD

Medio / Canal	**Acción específica**
Impreso	Imprimir las políticas clave (uso de contraseñas, respaldo, incidentes) y colocarlas en lugares visibles (oficinas, sala de reuniones).
Correo institucional	Enviar boletines cortos explicando una política por semana con ejemplos.
Carpeta física de políticas	Mantener una copia firmada y accesible en Secretaría para consulta interna.
Charlas informativas	Breves sesiones de 15 minutos para explicar las nuevas reglas y aclarar dudas.
Grupo de WhatsApp interno	Enviar recordatorios o tips semanales sobre buenas prácticas de seguridad.

Acciones de Difusión

- Guía completa con las principales reglas de seguridad de la información.
- Guía rápida de actuación ante incidentes informáticos.
- Ejemplos visuales de correos electrónicos fraudulentos y contraseñas vulnerables, con fines educativos.
- Formulario de registro de asistencia y evaluación de conocimientos, disponible en formato físico o digital.

Resultados Esperados

- Fortalecimiento de la cultura organizacional en torno a la seguridad de la información.
- Disminución de vulnerabilidades asociadas a fallas humanas, como accesos no autorizados o pérdida de datos.
- Alineación operativa con las políticas institucionales en materia de tecnologías de la información.
- Avance sostenido en el nivel de madurez del dominio DSS05 según el marco de referencia COBIT 2019.

CAPÍTULO IV
RESULTADOS Y ANÁLISIS

Se espera que la organización cuente con un marco formal de gobernanza de TI que defina claramente los roles, responsabilidades y políticas, fortaleciendo la toma de decisiones tecnológicas, aumentando la seguridad y disponibilidad de la información institucional, y promoviendo una cultura organizacional donde el personal asuma activamente su rol en la protección y uso adecuado de los recursos tecnológicos.

La evaluación Delphi, mediante el marco COBIT 2019 permitió identificar el nivel de madurez actual en cinco procesos clave: APO01, APO03, APO12, APO13 y DSS05, a través de encuestas aplicadas a los responsables de TI, observación directa y el análisis de brechas, se estableció un diagnóstico sobre la situación actual de seguridad Se evaluaron los procesos de gestión informática, contrastando con los niveles objetivo sugeridos según el modelo de capacidad.

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, la herramienta PILAR reveló que múltiples salvaguardas se encontraban en niveles -L1 o LO (no implementadas).

Adicionalmente, se aplicó una prueba de Student para muestras pareadas entre los puntajes promedio por dominio en la primera y segunda ronda Delphi, en la Tabla XXX 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, en la tabla ste hallazgo fortalece la validez empírica del modelo propuesto para incrementar la madurez institucional.

Tabla XXX.
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

El análisis evidencia que el marco COBIT 2019 es una herramienta útil para diagnosticar y planificar la mejora de la gobernanza de TI, incluso en contextos con niveles iniciales muy bajos

de madurez, la combinación con la metodología Delphi no solo permitió consensuar las acciones correctivas con expertos, sino que también facilitó su validación empírica mediante pruebas estadísticas, confirmando el impacto positivo de las intervenciones propuestas, demostrando que una implementación estructurada y participativa puede contribuir significativamente al fortalecimiento institucional y a la alineación con estándares internacionales de gestión y seguridad de TI.

CONCLUSIONES

Se determinó que el GAD. Tufiño no cuenta con un marco de gobernanza claramente definido, lo que genera debilidades en la toma de decisiones tecnológicas, además, existe una ausencia de roles definidos y una escasa supervisión sobre el uso de las tecnologías de la información (TI).

No está determinado qué sistemas tecnológicos apoyan a los diferentes procesos institucionales, lo que afecta directamente la eficiencia, trazabilidad y automatización de las actividades clave dentro del GADP. Tufiño, no tienen una identificación, análisis ni tratamiento sistemático de los riesgos informáticos, lo que lo expone a incidentes que podrían ser prevenidos con una gestión adecuada.

Existe una escasa formalización de políticas que orienten la protección de la información, así como una falta de mecanismos de monitoreo que garanticen el cumplimiento de las medidas básicas de seguridad informática y no se cuenta con procedimientos claros para la atención de incidentes, monitoreo continuo de sistemas ni protocolos de respaldo que garanticen la continuidad operativa de los servicios tecnológicos.

Ademas, la aplicación del marco COBIT 2019, mediante factores de diseño junto con la metodología Delphi, demostraron ser una herramienta eficaz para evaluar y fortalecer la gobernanza de tecnologías de la información en instituciones públicas, en el caso del GAD Tufiño, se logró identificar brechas sustanciales entre los niveles actuales y objetivos, particularmente en dominios críticos como la gestión de incidentes (DSS05) y la seguridad de la información (APO13).

Gracias a un proceso iterativo de validación, se alcanzó una mejora del 8 %, pasando de un 92 % a un 100 % de aceptación de la propuesta por parte de los expertos, lo que evidencia la efectividad de las medidas implementadas.

Los hallazgos de este estudio subrayan la necesidad de la mejora continua y la gobernanza adaptativa para alinear los procesos de TIC con los objetivos estratégicos, al aprovechar el enfoque estructurado de COBIT 2019, las instituciones educativas pueden mejorar su eficiencia, seguridad y la madurez general de la gobernanza de las TIC.

RECOMENDACIONES

Con base en los resultados de la evaluación de la madurez de la seguridad informática y los dominios analizados, se plantean las siguientes recomendaciones orientadas a fortalecer la gobernanza de TI en la institución y asegurar la sostenibilidad de las mejoras implementadas:

En el dominio APO01, se recomienda definir formalmente los roles, responsabilidades y procesos relacionados con la toma de decisiones en tecnologías de la información. Esto implica establecer políticas claras, comunicarlas adecuadamente al personal e implementar mecanismos de supervisión desde la alta dirección para asegurar su cumplimiento.

Para el dominio APO03, es aconsejable documentar y alinear los procesos institucionales a través de la elaboración de un mapa de procesos actualizado, que los clasifique como estratégicos, operativos o de apoyo, y los asocie con las tecnologías que los respaldan, facilitando así la trazabilidad y la eficiencia de la gestión institucional.

En cuanto al dominio APO12, se sugiere implementar un sistema formal de gestión de riesgos de TI, mediante una matriz institucional que evalúe la probabilidad e impacto de los riesgos identificados, contemple medidas específicas de mitigación y sea revisada periódicamente para garantizar su vigencia.

Con respecto al dominio APO13, se recomienda adoptar y formalizar políticas de seguridad informática relacionadas con el uso de contraseñas, software autorizado, navegación segura y protección de archivos, acompañadas de programas de capacitación al personal para garantizar su correcta aplicación y fomentar una cultura organizacional orientada a la seguridad.

En el ámbito del dominio DSS05, es fundamental fortalecer la seguridad operativa mediante la elaboración de un plan de respuesta ante incidentes, la realización regular de respaldos de la información, el mantenimiento actualizado de los sistemas antivirus y la implementación de monitoreo continuo de los sistemas críticos, con el objetivo de garantizar la continuidad de los servicios tecnológicos.

Además, se recomienda incorporar el dominio MEA01, a fin de establecer procesos de monitoreo, evaluación y auditoría interna que permitan dar seguimiento a las acciones implementadas y asegurar la mejora continua en materia de seguridad y gobernanza de TI.

Finalmente, se sugiere que las políticas de seguridad desarrolladas durante este proyecto se adopten como base para futuras evaluaciones periódicas de madurez institucional. Dado que

el proyecto es replicable, se recomienda también su aplicación en otras dependencias o instituciones con características similares, contribuyendo así a la estandarización de las prácticas de gobernanza y seguridad informática alineadas con los marcos internacionales.

BIBLIOGRAFÍA

[1] D. Utomo, M. Wijaya, S. Suzanna, E. Efendi y N. T. M. Sagala, «Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A,» *CommIT (Communication and Information Technology) Journal*, vol. 16, n.º 2, págs. 129-141, 2022.

[2] E. Ritegno, *COBIT es el marco de trabajo reconocido a nivel mundial, que ayuda a garantizar el Gobierno Corporativo de la Información y la Tecnología (GEIT)*, 2019. dirección: https://www.studocu.com/ec/document/university-of-the-armed-forces/business-management-sl/cobit-2019-implementation-guide-res-spa-0719/86391336.

[3] G. Morris, W. Tangka y E. Lompoliu, «Enhancing IT Governance at BPS Manado: A COBIT 2019 Framework Implementation Study (Peningkatan Tata Kelola TI di BPS Manado: Kajian Implementasi Framework COBIT 2019),» *Teika Journal*, vol. 14, n.º 1, 2023. doi: 10.36342/teika.v14i1.3325. dirección: https://jurnal.unai.edu/index.php/teika/article/view/3325.

[4] N. H. Haay y M. N. Sitokdana, «Analysis of information technology governance on communication and information service of Papua province using COBIT 2019,» *Journal of Information Systems and Informatics*, vol. 4, n.º 2, págs. 349-360, 2022.

[5] A. Ishlahuddin, P. W. Handayani, K. Hammi y F. Azzahro, «Analysing IT governance maturity level using COBIT 2019 framework: A case study of small size higher education institute (XYZ-edu),» en *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, IEEE, 2020, págs. 236-241.

[6] 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, n.º 2, jun. de 2023.

[7] G. de Ecuador, *Plan de Desarrollo para el Nuevo Ecuador 2024-2025*, Consultado el 29 de enero de 2025, 2024. dirección: https://www.planificacion.gob.ec/plan-de-desarrollo-para-el-nuevo-ecuador-2024-2025/.

[8] Y. B. Dionisius y D. N. Utama, «Evaluation of the Implementation of Business Continuity Management Using COBIT 2019 Framework in Public Sector,» *Journal of System and Management Sciences*, vol. 13, n.º 2, págs. 409-427, 2023.

[9] C. J. Prasca Aya, A. M. Suárez Iguarán et al., «Modelo de gobierno y gestión de TI para desplegar la política de gobierno digital en las entidades tipo gobernación caso de estudio: Gobernación del Atlántico,» 2019. dirección: https://manglar.uninorte.edu.co/handle/10584/10156#page=1.

[10] E. Amore, T. Dilger, C. Ploder, R. Bernsteiner y M. Mezzenzana, «Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study,» *KnE Social Sciences*, págs. 73-101, 2023.

[11] J. Lainhart et al., *Cobit® 2019 Framework: Introduction & Methodology. COBIT: Control Objectives for Information and Related Technology, ISACA Publication*, 2023. dirección: https://shorturl.at/8LHfB.

[12] A. A. Cortés Fuentes, «Propuesta de método basado en COBIT 2019, para la evaluación de procesos tecnológicos en la municipalidad de Carrillo,» *InterSedes*, vol. 24, n.º 49, págs. 277-306, 2023.

[13] D. F. Quinteros Mendoza y W. A. Rodríguez Reátegui, «Modelo de madurez COBIT-2019 y su relación con los procesos de TI en el Gobierno Regional de San Martín, 2022,» 2023. dirección: https://www.scopus.com/authid/detail.uri?authorId=57312439700.

[14] J. C. Torregroza Rodríguez, «Gobierno de TIC y sus beneficios para organizaciones pequeñas,» Mes de 2023, URL: https://repository.unipiloto.edu.co/handle/20.500.12277/13070.

[15] C. Wijaya, M. Sukamto, R. Yunis y M. Megawati, «Audit tata kelola ti menggunakan cobit 2019 domain apo-12 pada universitas mikroskil,» *Jurnal SIFO Mikroskil*, vol. 24, n.º 2, págs. 197-210, 2023.

[16] J. A. Monsalve-Pulido, F. A. Aponte-Novoa y D. F. Chaves-Tamayo, «Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia),» *Revista facultad de Ingeniería*, vol. 23, n.º 37, págs. 65-72, 2014.

[17] R. Vargas Borbúa, L. Recalde Herrera et al., «Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa,» *URVIO Revista Latinoamericana de Estudios de Seguridad*, n.º 20, págs. 31-45, 2017.

[18] S. C. I. Simatupang y M. I. Fianty, «Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry,» *G-Tech: Jurnal Teknologi Terapan*, vol. 7, n.º 4, págs. 1391-1400, 2023.

[19] A. Algiffary, M. I. Herdiansyah e Y. N. Kunang, «Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI,» *Journal of Applied Computer Science and Technology*, vol. 4, n.º 1, págs. 19-26, 2023.

[20] L. H. Collante, A. Pranolo y A. P. Wibawa, «Implementation plan of the information security management system based on the NTC-ISO-IEC 27001: 2013 standard and security risk analysis. Case study: Higher education institution,» *Transactions on Energy Systems and Engineering Applications*, vol. 5, n.º 2, págs. 1-20, 2024.

[21] M. Gehrmann, «Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations,» *Navus-Revista de Gestão e Tecnologia*, vol. 2, n.º 2, págs. 66-77, 2012.

[22] D. A. M. José, D. S. Dupski y K. Amilkar, «Framework for Security Risk Assessment (FSRA) and Fuzzy Risk Inference System (FRIS) based on Standard ISO/IEC 27002: 2022,» *Revista de Informática Teórica e Aplicada*, vol. 31, n.º 2, págs. 43-55, 2024.

[23] T. S. Chimborazo Morocho, «Incidencia del gobierno de TI en la gestión estratégica de los GADs municipales de Cañar, Tambo y Suscal,» 2022. dirección: https://dspace.ucacue.edu.ec/server/api/core/bitstreams/0ce713dc-3589-4fc1-a43c-457e6365a310/content.

[24] S. Yakubu, «Book Review: Abdulrahman OSHIOKE ARUNAH, A history of Auchi Kingdom, Ilorin, Haytee Press and Publishing Co. Nig. Ltd, 2010, pp. 368, ISBN 976-8090-25-7,» *Eximia*, vol. 4, n.º 1, págs. 60-62, 2022.

[25] C. C. Berdejo Blanco et al., «Diseño de un modelo de gobierno y gestión de TI para las alcaldías municipales de sexta categoría: caso de estudio, Alcaldía de Sabanagrande,» 2023. dirección: https://manglar.uninorte.edu.co/handle/10584/11343#page=.

[26] E. M. Estébanes y J. C. G. Cano, «Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0,» *Ecorfan Journal*, vol. 2, n.º 5, págs. 109-131, 2011.

[27] L. Jaime y J. Barata, «How can FLOSS Support COBIT 2019? Coverage Analysis and a Conceptual Framework,» *Procedia Computer Science*, vol. 219, págs. 680-687, 2023.

[28] P. Năstase, F. Năstase y C. Ionescu, «Challenges Generated By the Implementation of the IT Standards COBIT 4.1, ITIL V3 and ISO/IEC 27002 in Enterprises.,» *Economic computation & economic cybernetics studies & research*, vol. 43, n.º 3, 2009.

[29] ISACA, *Guía de diseño COBIT® 2019: Diseño de una solución de Gobierno de Información y Tecnología*. Schaumburg, IL, USA: ISACA, 2019, isbn: 978-1-60420-793-4. dirección: https://www.isaca.org.

[30] R. F. Mubarak y M. I. Fianty, «Leveraging COBIT 2019 to Implement IT Governance in Mineral Mining Company,» *Journal of Information Systems and Informatics*, vol. 5, n.º 3, págs. 1058-1071, 2023.

[31] T. Wulyatiningsih, W. G. Mokodaser y J. Y. Mambu, «Information Technology Governance Analysis Using COBIT 2019 Framework at Bank Mandiri Girian Bitung Branch,» *J. Inf. Syst. Informatics*, vol. 6, n.º 2, págs. 865-881, 2024.

[32] A. L. Ayu, M. Lubis, L. Abdurrahman, I. F. Zamzami, R. A. Alqahtani y R. Ramadhani, «Assessment of IT Risk Management at the Faculty of Industrial Engineering, Telkom University, Utilizing the COBIT 2019 Framework's APO12 Domain with LAM INFOKOM Standards Mapping,» *Electronic Integrated Computer Algorithm Journal*, vol. 1, n.º 2, págs. 50-56, 2024.

[33] J. Y. Mambu, R. J. Lontaan, E. Lompoliu, J. Salindeho y J. Sambul, «IT GOVERNANCE CAPABILITY LEVEL IDENTIFICATION OF COBIT 2019 AT THE RSUP PROF. DR. RD KANDOU, MANADO, NORTH SULAWESI,» dirección: https://shorturl.at/NCqyG.

[34] M. Kesuma, R. H. Saputra, M. A. Syaputra, J. Fitra y M. R. Romahdoni, «Design Of Information Technology (IT) Governance Using Framework Cobit 2019 Subdomain APO01 (Case Study: Instidla),» *J. Teknol. Komput. dan Sist. Inf*, vol. 5, n.º 3, págs. 157-162, 2022.

[35] F. E. Larasati, A. Kusumawati y R. A. S. Prayoga, «ANALISIS LEVEL PENGELOLAAN SI/TI DI DINAS KESEHATAN PROVINSI JAWA TIMUR BERDASARKAN FRAMEWORK COBIT 2019,» *Journal of Computer Science and Information Technology*, vol. 1, n.º 2, págs. 110-127, 2024.

[36] L. N. Amali, M. R. Katili y S. Suhada, «Core model of information technology governance system design in local government,» *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, n.º 4, págs. 750-761, 2023.

[37] M. K. Anam, S. D. Putri, D. Yuliana, E. Yumami y T. P. Lestari, «Application Of the Cobit 2019 Framework to Analyse the Security Of Academic Information Systems,» *Decode: Jurnal Pendidikan Teknologi Informasi*, vol. 3, n.º 2, págs. 296-309, 2023.

[38] A. Nisri, «Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019,» *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, vol. 9, n.º 1, págs. 34-41, 2023.

[39] L. Atrinawati, E. Ramadhani, T. Fiqar et al., «Assessment of process capability level in university XYZ based on COBIT 2019,» en *Journal of Physics: Conference Series*, IOP Publishing, vol. 1803, 2021, pág. 012 033.

[40] D. J. Tipán Oscullo, «Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1. 1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones–Corporación Nacional de Telecomunicaciones.,» 2023. dirección: https://shorturl.at/6nLuC.

[41] E. Martínez y J. Garcia, «Sistemas informaticos de innovacion empresarial,» *Revista ECORFAN*, vol. 2, n.º 5, págs. 109-131, 2011.

[42] C. C. Nacional, *PILAR: Herramienta de Análisis de Riesgos*, https://www.ccn-cert.cni.es, Disponible en: https://www.ccn-cert.cni.es/seguridad/pilar.html, 2020.

ANEXOS

ANEXO N° 1 Matriz de validación método DELPHI

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

SUBDECANATO

MATRIZ DE VALIDACIÓN MÉTODO DELPHI

El presente instrumento es el trabajo de integración curricular previo a la obtención del título de INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN, titulado "EVALUACIÓN DE LA MADUREZ DE SEGURIDAD INFORMÁTICA Y PROPUESTA DE MEJORAS PARA UN GOBIERNO AUTÓNOMO DESCENTRALIZADO PARROQUIAL RURAL DE TUFIÑO: UNA APROXIMACIÓN BASADA EN COBIT 2019".

A continuación, se presenta el sistema de objetivos de la investigación, cuyo propósito es proporcionar información relevante para la evaluación de la aplicación del estándar COBIT 2019, en el marco de la propuesta del Plan de Mejoras.

Objetivo general

Realizar una evaluación de la madurez de seguridad informática y propuesta de mejoras para un Gobierno Autónomo Descentralizado Parroquial Rural De Tufiño: una aproximación basada en COBIT 2019.

Objetivo Específico

Evaluar el plan de seguridad desarrollado a través expertos mediante el método de Delphi, verificando el cumplimiento de los dominios del estándar COBIT 2019 para optimizar la resiliencia ante amenazas.

INSTRUMENTO DE EVALUACIÓN – MODELO DE MADUREZ COBIT 2019

Por favor, indique el nivel de madurez que mejor representa su evaluación del cumplimiento del objetivo evaluado en la organización, de acuerdo con el modelo COBIT 2019.

Marque con una "X" el nivel correspondiente.

Niveles de Madurez según COBIT 2019

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 Optimización	El proceso se mejora continuamente basado en datos y análisis de desempeño.

Evaluación por Dominio COBIT

COBIT 2019	Criterio de Evaluación	1	2	3	4	5	Observaciones / Sugerencias
APO01	**Gestión del Marco de Gobernanza**						
Debilidad detectada:	No existe una estructura formal para la toma de decisiones tecnológicas.						
Política Sugerida	1. Uso de contraseñas y actualizaciones periódicas.						
	2. Prohibición al compartir cuentas y contraseñas.						
	3. Instalación de software no autorizado.						
	4. Uso restringido de dispositivos USB personales.						
	5. Almacenamiento y respaldo de archivos de trabajo.						
	6. Uso de internet con fines laborales.						
	7. Reporte de anomalías y fallas informáticas.						
	8. Política de Gobernanza y Roles de TI.						

	9. Política de Uso Aceptable y Responsabilidades del Usuario Final.						
	Definición de roles, responsable TI y estructura de gobernanza						
APO03	Gestión de la Arquitectura Empresarial						
Debilidad detectada:	No se tiene claro qué sistemas o equipos se usan para qué procesos.						
Política Sugerida	1. Diseño de procesos centrados en el usuario						
	2. Documentación y mantenimiento del mapa de procesos						
	3. Gestión de tecnologías alineadas a los procesos						
	4. Atención ciudadana multicanal y eficiente						
	5. Mejora continua e innovación						
APO012	**Gestión de Riesgos**						
Debilidad detectada:	No hay gestión activa de riesgos informáticos						
Política Sugerida	1. Identificación sistemática de riesgos de TI						
	2. Registro y evaluación de riesgos						
	3. Acciones de mitigación y responsables						
	4. Sensibilización y capacitación						
APO013	**Gestión de Seguridad**						
Debilidad detectada:	Faltan políticas básicas de seguridad y protección de datos.						
Política Sugerida	1. Buenas Prácticas para Contraseñas y Uso de Dispositivos Contraseñas Seguras.						
	2. Uso Responsable de Equipos y Dispositivos						

	3. Uso del Correo Electrónico y Navegación						
	4. Guardar archivos en lugares seguros						
	5. Proteger el acceso a los archivos						
	6. Evitar riesgos comunes						
	7. Realizar respaldos periódicos						
DSS05	**Gestión de Servicios de Seguridad**						
Debilidad detectada:	No hay un plan claro para actuar ante incidentes						
Política Sugerida	1. Ataque Informático Detectado (virus, phishing, acceso no autorizado)						
	2. Caída del Sistema o de Algún Programa						
	3. Pérdida de Datos o Archivos Importantes						

Sección de Valoración Global - COBIT 2019

1. **¿Considera que el plan propuesto cubre de forma integral los dominios relevantes de COBIT 2019 en materia de seguridad?**

   ☐ Sí ☐ Parcialmente ☐ No

2. **¿Está claramente definida la estructura de gobernanza y sus roles en relación con la seguridad de la información (APO01)?**

   ☐ Sí ☐ Parcialmente ☐ No

3. **¿El plan incluye una arquitectura empresarial de TI alineada con principios de seguridad y documentación adecuada (APO03)?**

   ☐ Sí ☐ Parcialmente ☐ No

4. **¿Considera que el análisis y gestión de riesgos fue realizado con un enfoque riguroso y metodológico (APO12)?**

   ☐ Sí ☐ Parcialmente ☐ No

5. **¿Las políticas y controles de seguridad del plan promueven la confidencialidad, integridad y disponibilidad de la información (APO13)?**

   ☐ Sí ☐ Parcialmente ☐ No

6. **¿Se contemplan medidas adecuadas de monitoreo, detección y respuesta ante incidentes de seguridad (DSS05)?**

   ☐ Sí ☐ Parcialmente ☐ No

¿Qué aspectos considera que deben mejorarse o reforzarse en el plan propuesto?

.....

.....

_____

Datos del Evaluador