Pontificia Universidad Católica del Ecuador
FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE

PUCE

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI

PROPUESTA DE MODELO DE PLANEACIÓN ESTRATÉGICA DE TICS-GOBERNANZA CON COBIT PARA EMPRESAS DEL SECTOR FINANCIERO BANCARIO EN EL ECUADOR, UN ENFOQUE EJEMPLAR EN UNA INSTITUCIÓN FINANCIERA.

Autor: Jazmín del Rocío Torres Guerrero

Director: Damián Aníbal Nicolalde Rodríguez

Quito-Ecuador, 2024.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, JAZMÍN DEL ROCÍO TORRES GUERRERO, con CI 1725167850, autor del trabajo de graduación PROPUESTA DE MODELO DE PLANEACIÓN ESTRATÉGICA DE TICS-GOBERNANZA CON COBIT PARA EMPRESAS DEL SECTOR FINANCIERO BANCARIO EN EL ECUADOR, UN ENFOQUE EJEMPLAR EN UNA INSTITUCIÓN FINANCIERA. previa la obtención del título profesional de Magíster en Tecnologías de la Información con mención en Gestión y Administración de TI, en la Facultad de Ingeniería

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENECYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de información de la Educación Superior del Ecuador para su difusión pública respetando los derechos del autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: "PROPUESTA DE MODELO DE PLANEACIÓN ESTRATÉGICA DE TICS-GOBERNANZA CON COBIT PARA EMPRESAS DEL SECTOR FINANCIERO BANCARIO EN EL ECUADOR, UN ENFOQUE EJEMPLAR EN UNA INSTITUCIÓN FINANCIERA", presentado por el maestrante TORRES GUERRERO JAZMÍN DEL ROCÍO, titular de la Cédula de Identidad Nº 1725167850 para optar al Grado de Magíster en Educación mención gestión del aprendizaje mediado por TIC, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ciencias de la Educación.

En la ciudad de Quito, a los 15 días de abril de 2024

_____

DAMIAN ANIBAL NICOLALDE RODRIGUEZ C.I. 1715641716

danicolalde@puce.edu.ec

NRO TELEFONO: 0984279611

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 6 % índice de similitud con otras fuentes.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

AGRADECIMIENTO

Dios, te doy gracias por tu misericordia y por guiar mi vida. Gracias por permitirme vivir esta experiencia de vida, por los milagros que realizas y por tu amor incondicional. Te agradezco por escucharme; tu luz me guía en cada paso que doy. Eres lo más poderoso que tengo. Gracias porque me permitiste conocerte cuando era muy joven, lo cual cambio mi vida para siempre, A menudo, nosotros los humanos hablamos contigo para pedirte cosas, para que nos cambies y nos bendigas y eso está muy bien; pero hoy quiero simplemente hablar contigo para decirte: GRACIAS.

Ma (Rocío Guerrero), Pa (Jorge Torres), ñaños (Maribel y Jorge Torres), Amor (Bryan Nuñez), nuestra amada *Mamita Lida*, quien nos mira desde el cielo *Abuelita (1940-2023))*, ustedes son mi motor, nada tiene sentido sin ustedes, nada tiene sentido sin su amor, gracias por guiarme por ser mi apoyo, cada uno de ustedes cumple un papel crucial en mi vida, son lo más importante y de los regalos más bonitos. A lo largo de todos mis proyectos ustedes están presentes deseándome lo mejor y ayudándome. Que Dios nos permita seguir disfrutando juntos de esta hermosa vida. Y a ti, Mamita Lida, te pido que nos cuides desde el cielo.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

DEDICATORIA

Para Lida Viteri (1940-2023)

Quiero dedicar este trabajo de titulación a mi amadísima abuelita, Mamita Lida, a quien considero mi segunda madre. Hoy deseo expresar al mundo que, gracias a ti, estoy aquí y he llegado a ser quien soy. Estabas presente cuando comencé esta maestría, y aunque lamentablemente partiste antes de verme concluir, estoy profundamente agradecida con Dios por haberme permitido disfrutar de tantos momentos maravillosos a tu lado, llenos de alegría, tristeza, diversión, aburrimiento y singularidad. Gracias por luchar valientemente contra tu enfermedad. Aprendí mucho de tu tenacidad y deseo de vivir; diría que incluso ganaste, superando las estadísticas. Viviste muchos milagros, y fuiste un milagro en mi vida. No todos tienen la fortuna de conocer a alguien como tú. Has dejado una huella imborrable en la vida de muchas personas, quienes al recordarte piensan en lo buena, amable, amorosa, dedicada, bondadosa y generosa que fuiste. Dejaste un legado hermoso, y mi sueño es dejar ese legado. Siempre mis logros también eran tuyos, y eso sigue siendo así. Sé que tu tiempo en este mundo terrenal simplemente llegó a su fin y que ahora, simplemente te transformaste ante la presencia de Dios, puedes verme, escucharme y guiarme desde donde estás. Te extraño mucho ML.

Pst: *Gracias por todo, visítame en los sueños.*

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

PROPUESTA DE MODELO DE PLANEACIÓN ESTRATÉGICA DE TICS-GOBERNANZA CON COBIT PARA EMPRESAS DEL SECTOR FINANCIERO BANCARIO EN EL ECUADOR, UN ENFOQUE EJEMPLAR EN UNA INSTITUCIÓN FINANCIERA

INFORME DE ORIGINALIDAD

6%	5%	2%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.hindawi.com Fuente de Internet	<1%
2	Submitted to Universidad Gerardo Barrios de El Salvador Trabajo del estudiante	<1%
3	www.inclusion.gob.ec Fuente de Internet	<1%

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo JAZMIN DEL ROCIO TORRES GUERRERO, con cédula de identidad # 1725167850, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; se ha consultado las referencias bibliográficas que se incluyen en el presente documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a esté trabajo, a la PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

ÍNDICE DE CONTENIDOS

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

PROPUESTA DE MODELO DE PLANEACIÓN ESTRATÉGICA DE TICS-GOBERNANZA CON COBIT PARA EMPRESAS DEL SECTOR FINANCIERO BANCARIO EN EL ECUADOR, UN ENFOQUE EJEMPLAR EN UNA INSTITUCIÓN FINANCIERA.

Autor: Jazmín del Rocío Torres Guerrero

Director -Tutor: Damián Aníbal Nicolalde Rodríguez

Fecha: 2024/04/15

RESUMEN

Este estudio se centra en la creación de un marco de gobernanza para las Tecnologías de la Información (TICs) en el sector bancario financiero de Ecuador, utilizando el modelo COBIT (Control Objectives for Information and Related Technologies). La investigación destaca cómo COBIT puede estandarizar y mejorar la gestión de las TICs, utilizando un caso específico de una institución bancaria para demostrar la transformación en la administración de los recursos tecnológicos. La principal motivación de este estudio es desarrollar un modelo de planeación estratégica de TICs-gobernanza que no solo se alinee con los objetivos estratégicos de las instituciones financieras sino que también cumpla con los requisitos normativos, proteja la información y maximice el valor empresarial. La metodología aplicada en esta investigación combina técnicas cualitativas, incluyendo análisis descriptivo y revisión de documentos, artículos, y registros históricos complementados con observación directa. Este enfoque híbrido permite una comprensión profunda de la implementación del modelo COBIT dentro del contexto institucional específico del sector bancario ecuatoriano. Además, se realizó una exhaustiva recopilación de datos de fuentes secundarias para asegurar que el modelo propuesto fuera robusto y aplicable en el entorno local.

El modelo de planeación estratégica desarrollado se basa en las mejores prácticas establecidas por COBIT y está diseñado para ser flexible y adaptable a diferentes instituciones financieras,

considerando sus visiones, misiones y estrategias únicas. A través de este modelo, se propone una gobernanza de TIC que no solo mejora la eficiencia operativa sino que también fortalece la seguridad de la información y la conformidad regulatoria. Los resultados de la investigación muestran que la adopción de COBIT facilita una significativa mejora en la gobernanza y la gestión de las TICs, alineando estos recursos tecnológicos más estrechamente con los objetivos empresariales de las instituciones financieras. Se demostró que este enfoque puede reducir los riesgos asociados con la gestión de TICs y mejorar la protección de la información. Las recomendaciones del estudio incluyen la implementación de controles de riesgos y evaluaciones continuas para mantener y mejorar la gestión de TICs, adaptándose a los desafíos presentados por la digitalización y las cambiantes regulaciones financieras.

Este trabajo también discute la importancia de un marco de gobernanza eficaz para las TICs en el contexto de un sector financiero que está en constante evolución debido a la digitalización y las regulaciones emergentes. Se sugiere que las instituciones financieras adopten prácticas de gobernanza de TIC que no solo respondan a las necesidades operativas inmediatas sino que también promuevan el crecimiento y la sustentabilidad a largo plazo. En conclusión, el modelo propuesto ofrece una estructura integral para la planeación estratégica y la gobernanza de las TICs en el sector bancario financiero de Ecuador. Al implementar este modelo, las instituciones financieras pueden esperar no solo cumplir con los estándares regulatorios actuales sino también adaptarse de manera proactiva a los requisitos futuros, asegurando así que continúen prosperando en un ambiente competitivo y regulado. Las directrices de COBIT se han demostrado como fundamentales para este proceso, proporcionando un marco sólido que facilita la alineación estratégica y la eficiencia operativa.

Palabras clave: Planeación Estratégica de TIC's, Gobernanza de TIC's, TIC (Tecnologías de la Información y la Comunicación), COBIT (Control Objectives for Information and Related Technologies), Lean IT, TOGAF (The Open Group Architecture Framework), BSC (Balanced Scorecard)

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN
Y ADMINISTRACIÓN DE TI

PROPOSAL FOR A STRATEGIC PLANNING MODEL OF ICT-GOVERNANCE WITH COBIT FOR COMPANIES IN THE BANKING FINANCIAL SECTOR IN ECUADOR, EJEMPLO EN UNA INSTITUCIÓN FINANCIERA.

Autor: Jazmín del Rocío Torres Guerrero

Director -Tutor: Tutor: Damián Aníbal Nicolalde Rodríguez

Fecha: 2024/04/15

ABSTRACT

This study focuses on establishing a governance framework for Information Technologies (IT) in the financial banking sector of Ecuador, using the COBIT model (Control Objectives for Information and Related Technologies). The research highlights how COBIT can standardize and enhance IT management, utilizing a specific case of a banking institution to demonstrate the transformation in the administration of technological resources. The primary motivation of this study is to develop a strategic planning model for IT governance that not only aligns with the strategic objectives of financial institutions but also meets regulatory requirements, protects information, and maximizes business value. The methodology employed in this research combines qualitative techniques, including descriptive analysis and review of documents, articles, and historical records, complemented by direct observation. This hybrid approach allows for a deep understanding of the implementation of the COBIT model within the specific institutional context of the Ecuadorian banking sector. Furthermore, an exhaustive collection of data from secondary sources was conducted to ensure that the proposed model was robust and applicable in the local environment. The developed strategic planning model is based on COBIT's best practices and is designed to be flexible and adaptable to various financial institutions, taking into account their unique visions, missions, and strategies. Through this model, a governance of IT is proposed that not only improves operational efficiency but also

strengthens information security and regulatory compliance. The results of the research show that the adoption of COBIT significantly enhances IT governance, aligning these technological resources more closely with the business objectives of financial institutions. It was demonstrated that this approach could reduce the risks associated with IT management and improve information protection. Recommendations from the study include the implementation of risk controls and continuous assessments to maintain and enhance IT management, adapting to the challenges posed by digitalization and changing financial regulations. This work also discusses the importance of an effective IT governance framework in the context of a financial sector that is continually evolving due to digitalization and emerging regulations. It is suggested that financial institutions adopt IT governance practices that not only meet immediate operational needs but also promote long-term growth and sustainability. In conclusion, the proposed model provides a comprehensive structure for strategic planning and governance of IT in the Ecuadorian financial banking sector. By implementing this model, financial institutions can expect not only to meet current regulatory standards but also to proactively adapt to future requirements, ensuring that they continue to thrive in a competitive and regulated environment. COBIT's guidelines have proven to be fundamental to this process, providing a solid framework that facilitates strategic alignment and operational efficiency.

Keywords: Strategic Planning for ICTs, ICT Governance, ICT (Information and Communication Technologies), COBIT (Control Objectives for Information and Related Technologies), Lean IT, TOGAF (The Open Group Architecture Framework), BSC (Balanced Scorecard)

INTRODUCCIÓN

El presente proyecto tiene como finalidad desarrollar una propuesta de modelo de planeación estratégica de TICs-gobernanza con COBIT para empresas del sector financiero bancario en Ecuador, ilustrada a través de un ejemplo práctico en una institución financiera específica. Se busca que el modelo sea flexible y ajustable a la misión, visión, y estrategias, proporcionando así una metodología para la gestión y gobernanza de las tecnologías de la información. Este investigación responde a la necesidad de un marco de gobernanza que no solo promueva la alineación estratégica de las TICs con los objetivos de negocio, sino que también asegure el cumplimiento de las normativas, fortalezca la seguridad de la información y potencie el valor empresarial. Mediante un análisis cualitativo del sector financiero y la incorporación de las mejores prácticas de COBIT, esta tesis aspira a entregar un modelo adaptable, capaz de ser implementado por distintas instituciones financieras en Ecuador (Ramírez, 2013). La necesidad de este marco de gobernanza es crítica; según datos del Banco Central del Ecuador (2021), el 75% de las instituciones financieras en el país han reportado incidentes de seguridad cibernética en el último año, destacando la importancia de fortalecer la alineación estratégica de las TICs con los objetivos de negocio y asegurar el cumplimiento normativo (Banco Central. 2021). Mediante un análisis cualitativo y la adopción de las mejores prácticas de COBIT, esta tesis pretende ofrecer un modelo flexible y efectivo para mejorar la seguridad de la información y el valor empresarial.

De acuerdo con el último informe de seguridad del Banco Central de Ecuador, se registró un aumento del 30% en incidentes de seguridad cibernética en el sector financiero durante el 2022, subrayando la necesidad urgente de robustecer las estrategias de gobernanza de TICs (Banco Central del Ecuador, 2022)." El objetivo principal de esta investigación es elaborar una propuesta de modelo de planeación estratégica y gobernanza para las TICs utilizando el marco COBIT, adaptado para el sector bancario financiero en Ecuador. Este modelo, será aplicado como ejemplo a una institución financiera, busca estandarizar y optimizar las prácticas de gestión de las TICs. Al hacerlo, la investigación busca establecer un marco de gobernanza que facilite la alineación estratégica de las TICs con los objetivos generales de las instituciones financieras, asegure el cumplimiento con los estándares regulatorios, proteja la seguridad de la información y fomente la maximización del valor empresarial. Además, se busca identificar el Entorno del Sector Bancario Financiero en Ecuador como comprender a el panorama del sector

bancario financiero en Ecuador, incluidas las regulaciones y marcos legales relacionados, para adaptar el modelo a los requisitos específicos del contexto local. Este entendimiento servirá como base para asegurar que el modelo propuesto sea pertinente y efectivo dentro del ámbito regulatorio y operativo ecuatoriano.

Se propone identificar cuáles procesos de COBIT deberían implementarse como parte del marco de gobernanza y gestión de las TICs, junto con la implementación de un mapa de ruta respectivo. Esta selección estratégica de procesos permitirá que el modelo de gobernanza se alinee con los estándares mientras se adapta a las necesidades específicas del sector en Ecuador, y establecer las buenas prácticas y estándares generales para diseñar y aplicar el modelo de planeación estratégica de Tics-Gobernanza con COBIT, adaptado a entornos competitivos, exigentes y cambiantes. Esto incluye la adaptación de prácticas recomendadas por COBIT para asegurar que el modelo sea efectivo en promover una gobernanza y gestión de TICs resiliente y proactiva. También, de plantea proponer mecanismos de control de riesgos y evaluación continua para el control de riesgos, procedimientos, evaluación continua e indicadores o KPIs alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector bancario financiero en Ecuador. Esto permitirá un monitoreo y ajuste constantes del modelo, asegurando su relevancia y efectividad a largo plazo.

La investigación se basa en identificar el entorno del sector financiero bancario en Ecuador lo que implica comprender las regulaciones y marcos legales relacionados con la gobernanza de TIC´s en el país y en este sector en específico, incluyendo las regulaciones y marcos legales relacionados con la gobernanza de TIC´s, para adaptar el modelo a los requisitos específicos del contexto local. Al considerar las regulaciones locales, se asegura que el modelo cumpla con los estándares legales y pueda abordar los riesgos y desafíos particulares del sector financiero bancario en Ecuador.

Se analizará la utilización del COBIT (Control Objectives for Information and Related Technologies) con sus mejores prácticas reconocidas a nivel internacional como marco de gobernanza y gestión de TIC´s (ISACA, 2019). COBIT es un marco desarrollado por ISACA (Information Systems Audit and Control Association) que proporciona directrices y herramientas para el gobierno efectivo de las tecnologías de la información y los objetivos relacionados (Eito-Brun, Calleja Aliagam, 2020).

COBIT se basa en una serie de principios y procesos que abarcan desde la definición de metas y objetivos hasta la implementación de controles y la medición del desempeño. Estas mejores prácticas cubren aspectos claves de la gobernanza de TIC´s, como la alineación con los objetivos empresariales, la gestión de riesgos, el cumplimiento normativo, la seguridad de la información y la mejora continua.

Finalmente, se describen los procesos generales para diseñar y aplicar un modelo de planeación estratégica de TIC´s-Gobernanza con COBIT adaptado a entornos competitivos, exigentes y cambiantes como son las tecnologías que aplican inteligencia artificial. La investigación se concluye con la propuesta de controles de riesgos, procedimientos y evaluación continua alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector financiero bancario en Ecuador.

Además de los controles, se establecen procedimientos y procesos claros para la gestión de TIC´s en el sector financiero bancario, asegurando una gobernanza adecuada. Estos procedimientos abarcan aspectos como la planificación estratégica, la asignación de recursos, la gestión de proveedores, la gestión de incidentes y la gestión del ciclo de vida de los sistemas.

La evaluación continua es fundamental para garantizar la efectividad de los controles y procedimientos implementados. Se establecen mecanismos de monitoreo y medición para evaluar regularmente el desempeño de la gobernanza, identificar áreas de mejora y realizar ajustes necesarios. Esto garantiza una gobernanza efectiva, cumpliendo con las regulaciones y maximizando el valor empresarial en el entorno financiero.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

En el sector bancario ecuatoriano, a pesar de contar con modelos y estructuras de gestión de la información, se observan problemas significativos relacionados con la sostenibilidad y la adaptación ágil de estos modelos en situaciones de crecimiento inesperado de usuarios finales, lo que conduce a la sobrecarga de sistemas y modelos existentes. Además, la atención de incidentes en los servicios bancarios carece de procesos actualizados y alineados con la velocidad y calidad necesarias, resultando en largas filas y aglomeraciones, y la falta de aplicaciones y procesos de digitalización adecuados.

De esta problemática se derivan los siguientes problemas:

- Necesidad de Planeación Estratégica a Largo Plazo: Las instituciones bancarias requieren urgentemente el desarrollo de una propuesta actualizada de modelo de planeación estratégica de Tecnologías de la Información y Comunicación (TIC) y gobernanza con COBIT. Este modelo debe superar la planificación a corto plazo y enfocarse en una visión de largo plazo, con objetivos estratégicos que abarquen al menos diez años. Esto es esencial para adaptarse a los cambios y transformaciones en los sistemas bancarios, monetarios y financieros, impulsados por cambios tecnológicos cada vez más frecuentes y demandas crecientes de los clientes, que también requieren educación económica y financiera.
- **Retrasos y Falta de Actualización Normativa**: En el contexto del sector financiero bancario en Ecuador, incluyendo las regulaciones y marcos legales relacionados con la gobernanza con COBIT, se evidencian retrasos y una falta de actualización en la normativa vigente. Esto obstaculiza y dificulta la adaptación de un modelo alternativo que considere las dinámicas y requisitos específicos del entorno local.
- **Necesidad de Incorporar Buenas Prácticas Internacionales**: Es esencial analizar y aplicar las mejores prácticas internacionales reconocidas, como el marco de gobernanza y gestión de TIC COBIT, en las instituciones financieras ecuatorianas. Esto permitirá la incorporación de nuevos modelos y enfoques que mejoren la gestión y gobernanza de las TIC en estas organizaciones.

- **Desafíos en un Entorno Empresarial Competitivo:** En un entorno empresarial caracterizado por la competencia, la exigencia y los constantes avances tecnológicos, es fundamental disponer de un modelo de planeación estratégica de TIC y gobernanza que permita a las organizaciones del sector financiero adaptarse y mantenerse competitivas. Sin embargo, el diseño y la implementación efectiva de este modelo representan un desafío debido a la complejidad y dinamismo del entorno.

El problema principal radica en la necesidad de proponer mecanismos que permitan a las organizaciones del sector financiero controlar de manera efectiva los riesgos tecnológicos, establecer procedimientos adecuados para el manejo de la información y evaluar continuamente el desempeño de las prácticas implementadas. Estos mecanismos deben basarse en las mejores prácticas internacionales, como COBIT, y, al mismo tiempo, adaptarse a las particularidades y requisitos del sector financiero bancario en Ecuador.

En consecuencia, es esencial llevar a cabo un análisis exhaustivo de la utilización de COBIT y sus mejores prácticas reconocidas a nivel internacional como marco de gobernanza y gestión de TICs. Además, se deben describir los procesos generales para diseñar e implementar un modelo de planeación estratégica de TIC y gobernanza con COBIT que se adapte a entornos competitivos, exigentes y cambiantes, donde la inteligencia artificial y otras tecnologías desempeñan un papel fundamental. Este modelo deberá proponer controles de riesgos, procedimientos y una evaluación continua alineados con las mejores prácticas de COBIT y adaptados a las necesidades específicas del sector financiero bancario en Ecuador.

1.2. Objetivos de la Investigación

Objetivo General

1. Elaborar una propuesta de modelo de planeación estratégica de Tics-Gobernanza con COBIT para empresas del sector financiero bancario en el Ecuador, un enfoque ejemplar en una institución financiera.

Objetivos Específicos

1. Identificar el entorno del sector financiero bancario en Ecuador, incluyendo las regulaciones y marcos legales relacionados con la gobernanza con COBIT, para adaptar el modelo a los requisitos específicos del contexto local.
2. Determinar los procesos de COBIT a implementarse como marco de gobernanza y gestión de TIC´s junto a la implementación del respectivo road map.
3. Determinar las buenas práctica y estándares generales para diseñar y aplicar un modelo de planeación estratégica de Tics-Gobernanza con COBIT adaptado a entornos competitivos, exigentes y cambiantes.
4. Proponer mecanismos para control de riesgos, procedimientos, evaluación continua e indicadores o KPI alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector financiero bancario en Ecuador.

1.3. Justificación de la Investigación

El constante cambio de las Tecnologías de la Información y Comunicación, que incluye actualmente el espectacular desarrollo de la inteligencia artificial y sus múltiples aplicaciones, incentiva la redefinición de la estructura organizacional y funcionamiento del departamento de TI y del rol de los directivos, gerentes, CIO que dirigen las empresas del sector financiero bancario en el Ecuador. El constante cambio tecnológico genera un impacto positivo y un desafío para nuestras sociedades; el factor de adaptabilidad y la capacidad de desplegar herramientas de planeación estratégica de TIC´s es importante para asegurar su alineación con los objetivos empresariales, mejorar la competitividad, optimizar los recursos, gestionar los riesgos y mejorar la toma de decisiones en relación con la tecnología. Esto permitirá a las instituciones financieras aprovechar de manera efectiva el potencial de las TIC´s y lograr un crecimiento sostenible en un entorno empresarial cada vez más digitalizado.

La cultura de adaptabilidad y aplicación de modelos de planeación estratégica en instituciones bancarias debe ser primordial, por esta razón el presente proyecto consiste en proponer un modelo general de planeación estratégica de TIC´s-Gobernanza con COBIT que sea flexible y aplicable para la gestión del área de TI, se trata de una necesidad que existe al interior de las empresas del sector financiero para lograr mayor eficiencia, crecimiento y competitividad (Ramírez, 2013).

Siendo los bancos instituciones que regulan la vida económica de un país y constituyen un soporte de las unidades económicas familiares, empresariales, productivas, de servicios y a pesar que manejan tecnología necesitan procesos de capacitación y actualización en el talento humano de gerencia que asimile las dinámicas y demandas mundiales de la digitalización, la hiper comunicación y aplicación de la inteligencia artificial en las tecnologías de comunicación, en el marco de la gobernanza con COBIT.

Las empresas del sector financiero bancario en el Ecuador enfrentan desafíos en la adopción y gestión efectiva de las tecnologías de la información y comunicación, a menudo, carecen de una estructura organizacional de gestión de TIC´s adecuada y de un enfoque estratégico para su implementación y gobernanza. Esto limita su capacidad para aprovechar plenamente los beneficios que las TIC´s pueden proporcionar y conducir a una percepción errónea de que el área de TIC representa un gasto en lugar de un beneficio para el negocio. Por esto se plantea identificar el entorno del sector financiero bancario en Ecuador, incluyendo las regulaciones y marcos legales relacionados con la gobernanza de TICs, para adaptar el modelo a los requisitos específicos del contexto local.

1.4. Planteamiento del Problema

A pesar de contar con modelos y estructuras de gestión de la información, las instituciones bancarias presentan problemas de sostenibilidad y ágil adaptación de estos modelos ante diferentes situaciones como por ejemplo crecimientos no proyectados inusitados de usuarios finales, que finalmente desbordan los sistemas y los modelos planteados en los bancos.
En otro campo, por ejemplo, la ¨atención de incidentes en servicios bancarios¨ no presenta procesos de actualización y alineación de los soportes hacia los usuarios con la debida velocidad y calidad, por lo que usualmente se observan largas ¨filas¨ y aglomeraciones, no hay

las apps y los procesos de digitalización necesarios.
De esta discusión se identifican los siguientes problemas:
En las instituciones bancarias se requiere diseñar una propuesta actualizada de modelo de planeación estratégica de Tics-Gobernanza con COBIT, que logre superar la planificación de corto plazo poniendo énfasis en una visión con objetivos estratégicos a largo plazo, de por lo menos diez años, acorde con los cambios y las trasformaciones de los sistemas bancarios, monetarios y financieros que se suceden en el mundo y que están trasversalizados por cambios tecnológicos que se suceden cada vez en periodos más cortos que a su vez provocan demandas en el mercado de clientes a quienes también se debe brindar un soporte de educación económica y financiera.

En el entorno del sector financiero bancario en Ecuador, incluyendo las regulaciones y marcos legales relacionados con la gobernanza con COBIT, se puede apreciar retrasos y falta de actualización en la normativa que impiden o dificultan la adaptación de un modelo alternativo que tome en cuenta las dinámicas y los requisitos específicos del contexto local.

Es necesario analizar la utilización del COBIT con sus mejores prácticas reconocidas a nivel internacional como marco de gobernanza y gestión de TIC´s, con el objetivo de incorporar nuevos modelos en las instituciones financieras.

En un contexto empresarial caracterizado por la competencia, la exigencia y los constantes cambios tecnológicos, es fundamental contar con un modelo de planeación estratégica de Tics-Gobernanza que permita a las organizaciones del sector financiero adaptarse y mantenerse competitivas en el mercado. Sin embargo, el diseño y la aplicación efectiva de este modelo representan un desafío debido a la complejidad y dinamismo de estos entornos. Es necesario investigar y comprender los pasos y consideraciones clave que permitirán a las empresas del sector financiero diseñar y aplicar un modelo de planeación estratégica de Tics-Gobernanza con COBIT que se ajuste a sus necesidades específicas, les permita mantenerse competitivas y les brinde la capacidad de adaptarse rápidamente a los cambios tecnológicos y del mercado.

El problema radica en la necesidad de proponer mecanismos que permitan a las organizaciones del sector financiero controlar de manera efectiva los riesgos tecnológicos, establecer procedimientos adecuados para el manejo de la información y evaluar continuamente el desempeño de las prácticas implementadas. Estos mecanismos deben estar en línea con las

mejores prácticas establecidas por el marco de referencia y, al mismo tiempo, adaptarse a los requisitos y particularidades del sector financiero bancario en Ecuador.

Por lo tanto, es necesario analizar la utilización del COBIT con sus mejores prácticas reconocidas a nivel internacional como marco de gobernanza y gestión de TICs y se describirán los procesos generales para diseñar y aplicar un modelo de planeación estratégica de Tics-Gobernanza con COBIT adaptado a entornos competitivos, exigentes y cambiantes con tecnologías que aplican inteligencia artificial, proponiendo controles de riesgos, procedimientos y evaluación continua alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector financiero bancario en Ecuador.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Para el realizar el presente trabajo de titulación, se consideraron cuatro casos de estudio como antecedentes y referentes de investigación:

El artículo de Brum y Aliagam (2020) examina la incorporación de las prácticas de gestión documental en el marco del modelo COBIT y la visibilidad de las normas específicas de gestión de documentos ISO 15489 e ISO 30300 en dicho modelo. Se destaca que la gobernanza y gestión de servicios y sistemas de información cuentan con un conjunto de normas que reúnen las mejores prácticas desarrolladas por instituciones y empresas.

Estas experiencias se presentan en forma de marcos de referencia que establecen objetivos, indicadores y procesos, y que pueden ser utilizados como guía para definir los procesos internos y comparar el desempeño de las organizaciones con las mejores prácticas. Entre estos marcos de referencia destacan el modelo COBIT y la norma internacional ISO/IEC 38500, los cuales se enfocan en la gobernanza de las tecnologías de la información y comunicación (Eito-Brun, Calleja Aliagam, 2020).

El estudio realizado por Brum y Aliagam (2020) se centra en la integración de prácticas de gestión documental dentro del marco del modelo COBIT, un marco de referencia ampliamente utilizado para la gobernanza y gestión de servicios y sistemas de información en diversas organizaciones. Este artículo es relevante para el presente trabajo de titulación, que se enfoca en la creación de un modelo de planeación estratégica de TICs-Gobernanza con COBIT específicamente diseñado para empresas del sector financiero bancario en Ecuador.

El artículo proporciona una comprensión más profunda de cómo las prácticas de gestión documental pueden integrarse eficazmente en el marco de COBIT. Esto es crucial, ya que la investigación se centra en mejorar la gobernanza de las tecnologías de la información y comunicación en el contexto de las instituciones bancarias, lo que incluye la gestión eficiente de la documentación relacionada con las TIC, además, el estudio destaca la importancia de las normas específicas de gestión de documentos, como la ISO 15489 e ISO 30300, en el marco de COBIT, lo cual proporciona una orientación sobre las normativas clave que deben considerarse al desarrollar un modelo de gobernanza de TICs adaptado a las necesidades del

sector financiero bancario en Ecuador.

En el contexto de la investigación académica titulada *Identificaciones de los factores y eventos de riesgo operativo dentro del proceso de gestión de tecnologías de información y comunicaciones basado en COBIT 5.0 en instituciones financieras públicas, caso Banco del Estado* (Córdova, 2014)" de la Escuela Politécnica Nacional es relevante. El objetivo principal de este estudio es identificar los factores y eventos de riesgo operativo en el proceso de gestión de tecnologías de información y comunicaciones, considerando como factores de riesgo los procesos, personas, tecnología de la información y eventos externos. Esta tesis proporciona una visión detallada sobre los desafíos y las áreas críticas relacionadas con la gestión de tecnologías de información y comunicaciones en el sector financiero, lo que la convierte en una valiosa fuente de información para la investigación sobre este tema específico.

Además, esta investigación previa ofrece una contextualización detallada del problema al examinar los factores y eventos de riesgo operativo en la gestión de tecnologías de la información en instituciones financieras. Al basarse en COBIT 5.0, proporciona una comprensión práctica de la aplicación de este marco en un entorno bancario real. Los hallazgos y metodologías de esta tesis son valiosos para mi investigación, ya que me permiten entender cómo se identifican los factores de riesgo específicos en el contexto bancario ecuatoriano.

"La investigación sobre *La gestión de la tecnología de la información en la Unidad de Gestión de la Información de la Escuela Politécnica Nacional utilizando COBIT* (Velas tegui, Sanchez, 2007)." tiene información significativa para este trabajo de titulación. Esta investigación aplica metodologías y herramientas específicas del marco de referencia COBIT 3.0 para evaluar las prácticas de TI en la EPN. Al analizar la forma en la que estas teorías se implementan en un contexto práctico, es posible plantear ejemplos concretos y estudios de caso valiosos. Además, al comparar las operaciones existentes en la UGI con las pautas de COBIT 3.0, se tiene contexto para realizar una evaluación crítica que revelará áreas de mejora y proporcionará recomendaciones útiles para optimizar la gestión de TI en una organización específica. Este análisis no solo contribuye al conocimiento en el campo de la gestión de tecnología de la información, sino que también permite desarrollar habilidades esenciales en auditoría y evaluación de sistemas de TI (Velastegui. T, 2007).

El trabajo sobre la *Auditoría de riesgos informáticos en el departamento de Sistemas de Teleamazonas usando el marco COBIT* (Cordero & Ibujés, 2008)" de la Escuela Politécnica Nacional es de gran ayuda para el presente trabajo de titulación. En primer lugar, proporciona un enfoque práctico para aplicar COBIT en un contexto empresarial real, lo que permite entender cómo se implementa este marco en situaciones concretas. Además, el mapeo entre la Norma ISO 17799 y COBIT brinda una visión más amplia sobre cómo diferentes normativas se integran y se aplican en conjunto en el ámbito de las TI.

El uso de modelos de madurez y la metodología de COSO también ofrecen herramientas adicionales para evaluar la efectividad de los controles y los objetivos de control en un entorno específico. Al comprender cómo estos enfoques se aplican en el análisis de riesgos informáticos, puede ayudar a adaptar y aplicar estos conocimientos en el contexto del sector bancario.

Además, este trabajo presenta un informe final de auditoría que se genera como resultado del estudio lo que servirá como ejemplo práctico y proporcionará ideas sobre cómo estructurar y presentar los resultados de la presente investigación (Cordero. M & Ibujés. M. C, 2008).

2.2. Bases Teóricas.

Estos conceptos proporcionan una base teórica y conceptual para el planteamiento del modelo general de planeación estratégica de TIC´s-Gobernanza con COBIT para empresas del sector financiero bancario en el Ecuador.

2.2.1. Gobierno de Tecnologías de la Información (TI)

Las Tecnologías de la Información y Comunicación (TIC) se refieren a un conjunto de tecnologías que se utilizan para manejar y transmitir información. Estas tecnologías incluyen computadoras, software, redes, sistemas electrónicos, y tecnologías de telecomunicaciones como internet y sistemas de telefonía móvil. Las TIC engloban todas las tecnologías que facilitan la comunicación y el intercambio de información a través de medios electrónicos. Además, las tecnologías de vanguardia como la inteligencia artificial (IA) y la robótica son el avance de las TIC (Unacademy. 2023).

La gobernanza de TI representa el conjunto de procesos, estrategias y herramientas que las organizaciones emplean para optimizar el uso de la tecnología de la información, asegurando así el logro de objetivos y la mitigación de riesgos.

En el panorama empresarial actual, la tecnología de la información ha transformado radicalmente la forma en que se realizan los negocios a nivel global. Avances en comunicación, accesibilidad, automatización, análisis de datos y computación en la nube han creado un espectro casi infinito de posibilidades tecnológicas, sin embargo, es importante reconocer que las Tecnologías de la Información son un vehículo para alcanzar los objetivos dentro de una organización. Esto implica que, si la tecnología no está alineada con las metas empresariales, se convierte simplemente en una distracción sin propósito. Por este motivo, es crucial comprender a fondo el valor real de la gobernanza de TI para evitar desaprovechar el potencial tecnológico y garantizar que contribuya de manera significativa al éxito empresarial.

La gobernanza de TI orienta a las organizaciones en la gestión de sus tecnologías fundamentales, al implementase de manera efectiva, el gobierno de TI permite a las organizaciones administrar sus recursos tecnológicos con un propósito claro, esto implica asegurar que todas las plataformas, herramientas, estrategias e iniciativas de TI estén perfectamente alineadas y enfocadas en el logro de objetivos compartidos, además es parte integral del gobierno corporativo en su totalidad (García. H, 1016).

La implementación involucra procesos, estructuras organizativas y liderazgo que aseguran que la infraestructura de TI sostenga y refuerce las estrategias y objetivos generales de la organización. Esta responsabilidad no recae únicamente en el departamento de TI; más bien, es una responsabilidad conjunta de la dirección ejecutiva y la dirección de TI de la organización (Ojeda, 2008). En este contexto, la gobernanza de TI se convierte en un elemento vital para garantizar que la tecnología no solo sea poderosa, sino también relevante y significativa para el logro de los objetivos empresariales.

Normas, estándares y reglamentos asociados al gobierno de las TI

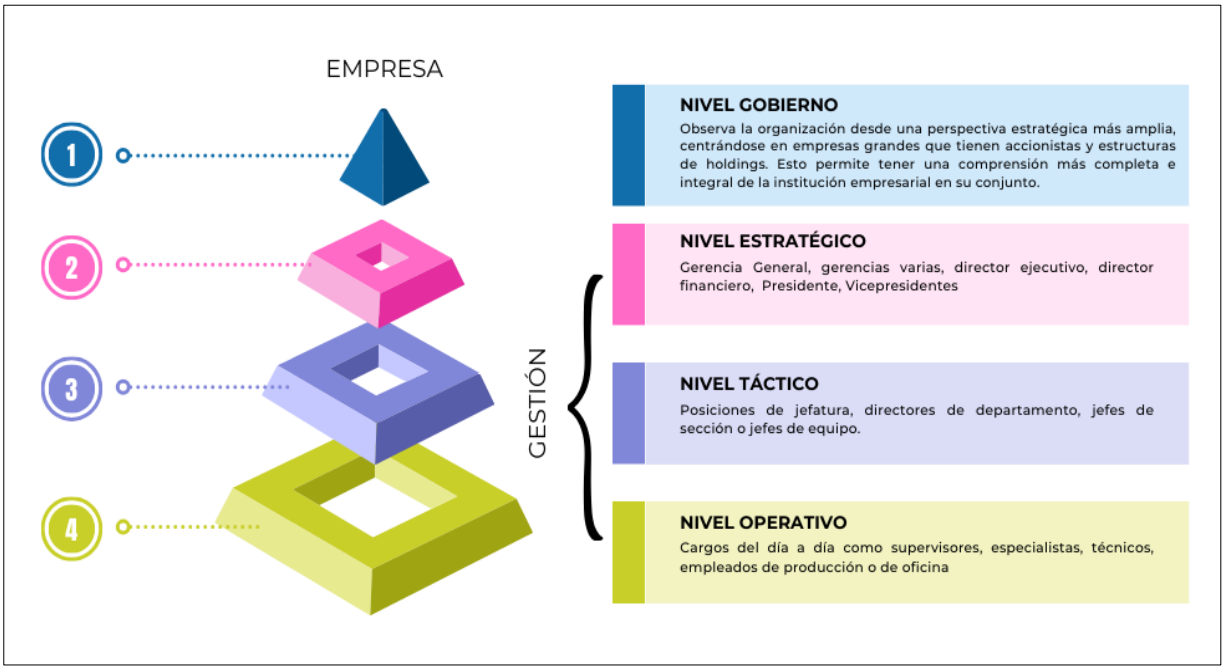
- **COBIT y el modelo de Gobernanza:** El principal propósito de este modelo y buena práctica es llevar a cabo el cumplimiento de los objetivos estratégicos de la organización a través de la implementación de marcos, normativas y buenas prácticas.

En términos generales, COBIT es un apoyo fundamental para alcanzar los objetivos de este modelo de gobernanza, no limitándose únicamente al ámbito de Tecnologías de la Información, sino también alineándose con el plan estratégico global de la institución, abarcando todas las facetas de la empresa, tales como la satisfacción del cliente, aspectos financieros, procesos operativos, así como el desarrollo humano y tecnológico (Arias. J, 2011).

Este enfoque de buenas prácticas se estructura sobre la base de dos pilares fundamentales: gobierno y gestión como se muestra en la siguiente figura 1:

Figura 1

Pirámide de Gobierno y Gestión.



Nota: Pirámide de Gobierno y Gestión en el cual se puede observar la subdivisión. Elaboración propia, 2023.

- **Gobierno:** Este componente se enfoca en el establecimiento de las políticas, estructuras organizativas y procesos necesarios para asegurar que las tecnologías de la información respalden y faciliten el logro de los objetivos estratégicos de la empresa. Implica una supervisión efectiva para garantizar la alineación de las actividades de TI con la visión global y los objetivos de la organización (Unacademy, 2023). La gobernanza debe:

✓ *Evaluar* y determinar objetivos balanceados y puntuales que las organizaciones,

empresas deben alcanzar.

- ✓ *Direccionar* a través de priorización y toma de decisión.
- ✓ *Monitorizar* el desempeño, conformidad y progreso en base a la dirección y objetivos establecidos (Rodrigues, N, 2023).

Se llega a la conclusión que las funciones principales de la gobernanza incluyen evaluar, direccionar y monitorizar. Esta descripción proviene directamente de COBIT, que la ha adoptado de la norma internacional de gobernanza ISO 38500.

- **Gestión:** En esta fase, se abordan las actividades cotidianas y los procesos operativos relacionados con las tecnologías de la información. La gestión adecuada implica la planificación, implementación, monitoreo y mejora continua de los sistemas de información, asegurando así que estos estén alineados con las metas organizativas y contribuyan de manera efectiva a su cumplimiento (Netmind., 2023).

En la implementación de prácticas de gobernanza de TI, se sigue un modelo estructurado basado en tres niveles, los cuales son comunes en muchas organizaciones y se utilizan para establecer una estructura sólida y efectiva para la gestión de la empresa (Velastegui. T, 2007).

- ✓ *Nivel Estratégico:* Se encuentra la dirección estratégica de la empresa. Aquí se toman decisiones de alto nivel que definen los objetivos y metas generales de la organización. En el contexto de la gobernanza de TI, esto implica decidir cómo la tecnología de la información puede ser utilizada para alcanzar los objetivos empresariales a largo plazo, las decisiones estratégicas incluyen la asignación de recursos, la definición de políticas generales y la garantía de que la tecnología de la información esté alineada con los objetivos de negocio.

- ✓ *Nivel Táctico:* Las decisiones estratégicas se traducen en planes y acciones concretas. Aquí se desarrollan los planes para alcanzar los objetivos estratégicos. En términos de gobernanza de TI, esto implica la planificación de proyectos específicos, la asignación de presupuestos detallados y la implementación de políticas y procedimientos específicos para garantizar que la tecnología se utilice de manera efectiva y eficiente, los gerentes de TI y otros líderes de equipos están principalmente involucrados en este nivel para garantizar que las estrategias se traduzcan en acciones prácticas.

- ✓ *Nivel Operativo:* Las decisiones tácticas se implementan y se llevan a cabo en las actividades diarias. Esto incluye la gestión cotidiana de los sistemas y recursos de TI, la supervisión de los proyectos en curso y la garantía de que las operaciones diarias estén alineadas con los objetivos estratégicos y tácticos de la organización. Aquí, los ingenieros, técnicos y otros profesionales de TI están altamente involucrados en mantener y operar sistemas, asegurando que las políticas y prácticas se sigan rigurosamente (Cordero. M & Ibujés. M, 2008). La gestión debe:

- ✓ *Planificar, construir, ejecutar y monitorizar* actividades que deben alinearse y ayudar en la conquista de los objetivos de la Gobernanza.

La gobernanza es responsabilidad de los ejecutivos (o consejo ejecutivo), y la gestión es responsabilidad de los gestores. Este modelo integral se convierte en una herramienta esencial para las empresas del sector financiero bancario en Ecuador, ya que permite una gobernanza efectiva y una gestión óptima de las tecnologías de la información. Al alinearse con las perspectivas clave de la organización, como las necesidades del cliente, la estabilidad financiera, los procesos operativos y el desarrollo del capital humano y tecnológico, esta práctica no solo mejora la eficiencia de TI, sino que también se traduce en un impacto positivo en la organización en su totalidad.

2.2.2. COBIT 5.0 (Control Objectives for Information and Related Technologies)

Definición

Es un marco de referencia desarrollado por ISACA que proporciona una guía para la gobernanza y gestión de las tecnologías de la información. COBIT ayuda a las organizaciones a establecer controles y procesos efectivos para maximizar el valor de las TIC y lograr los objetivos empresariales (García. H, 1016). Constituyen un conjunto de prácticas recomendadas que se despliegan a través de un marco de trabajo organizado en dominios y procesos. Este enfoque estructurado permite una gestión eficaz de las actividades relacionadas con la información y la tecnología.

Las mejores prácticas de COBIT son el resultado del consenso de expertos y se centran principalmente en establecer controles robustos en lugar de simplemente ejecutar tareas. Estas prácticas son cruciales para optimizar las inversiones en tecnología de la información,

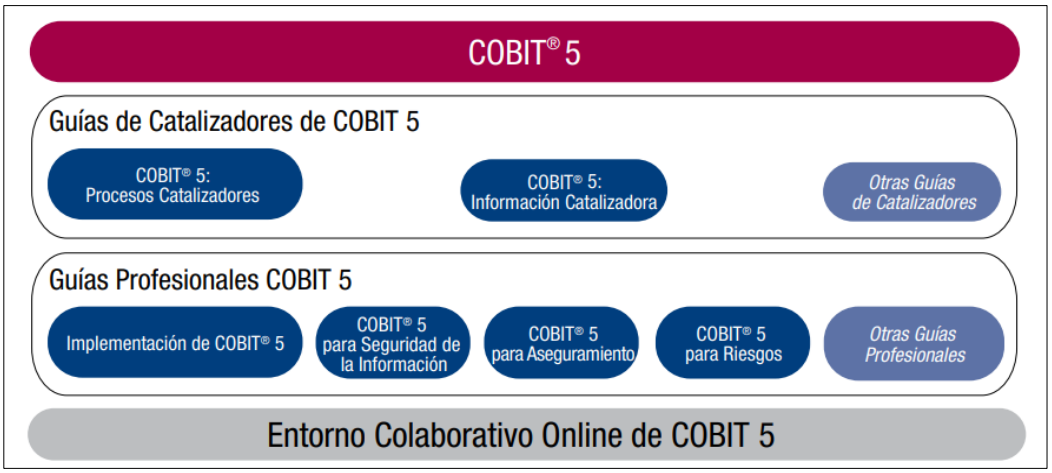
garantizar la entrega de servicios y proporcionar un estándar para evaluar el desempeño cuando las cosas no van como se esperaba.

Familia de Productos de COBIT 5.0

COBIT 5.0 se divide en 4 publicaciones como se muestra en la figura 2:

Figura 2

Familia de Productos de COBIT 5.0.



Nota: Familia de Productos de COBIT 5.0, desarrollada por ISACA ofrece un marco robusto para la gobernanza y gestión de TI, destacando por su capacidad para alinear los objetivos tecnológicos con las metas empresariales, por ISACA, 2012.

- **COBIT 5.0 Framework (Información Catalizadora):** Este producto describe el marco de trabajo. Proporciona una visión general de los principios y enfoques de COBIT 5.0 y cómo se pueden aplicar en la práctica.

- **COBIT 5.0 Guías de catalizadores:** Son una parte integral del marco de trabajo. Se centran en los "catalizadores", que son factores que pueden influir positivamente en la efectividad y eficiencia del gobierno y la gestión de las tecnologías de la información (TI). Incluyen aspectos como liderazgo, cultura y cambio organizativo, políticas y marcos de trabajo, y procesos.

  Las guías de catalizadores incluidas son las siguientes:

- ✓ Información Catalizadora*:* Tiene como objetivo proporcionar orientación adicional sobre cómo la información puede habilitar y potenciar las operaciones y la toma de decisiones en el contexto de COBIT 5.0.
- ✓ COBIT 5.0 Procesos catalizadores: Se centran en los procesos, incluyen áreas como la gestión de la información, la gestión de riesgos, la gestión de la seguridad, y otros procesos clave relacionados con las TI.

  Otras Guías de Catalizadores: Además de las dos mencionadas anteriormente, ISACA puede brindar otras guías de catalizadores para abordar aspectos específicos del gobierno y la gestión de TI.

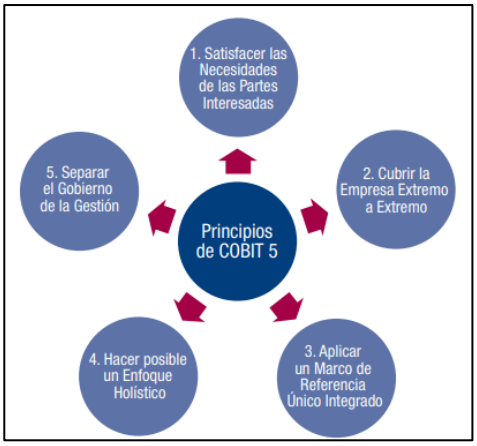
- **COBIT 5 Professional Guides:** Estas guías están diseñadas para profesionales de TI y ofrecen detalles técnicos y orientación específica para la implementación de COBIT 5.0 en diferentes contextos.
- **COBIT 5 Online:** ISACA ofrece herramientas y recursos en línea para ayudar a las organizaciones a evaluar su madurez en gestión de TI, realizar autoevaluaciones y acceder a recursos educativos.

Principios de COBIT

COBIT 5.0 se basa en cinco principios clave para el gobierno y la gestión de las TI empresariales las cuales se muestran en la Figura 3:

Figura 3

Principios de COBIT 5.0

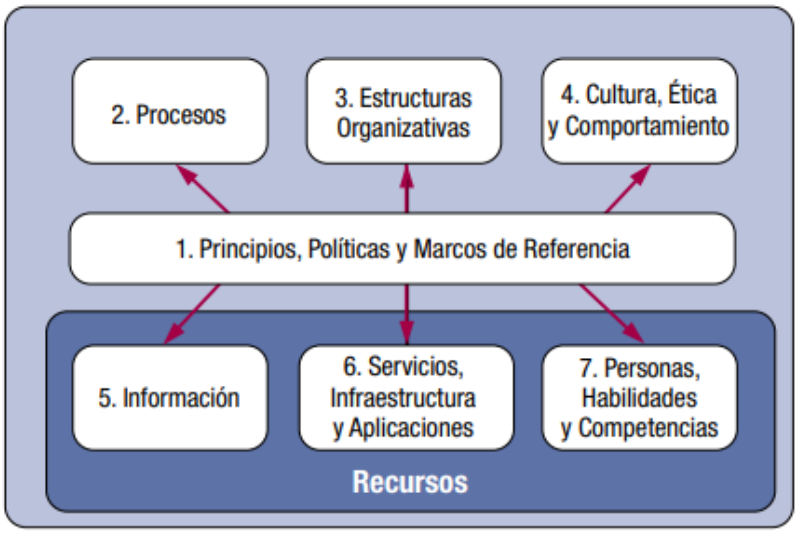


Nota: Principios de COBIT 5.0 Este marco promueve una integración efectiva entre las estrategias de TI y los objetivos corporativos, asegurando que las inversiones en TI generen valor, por ISACA, 2012.

1. **Satisfacer las Necesidades de las Partes Interesadas**: COBIT 5.0 permite a las empresas crear valor equilibrando beneficios, riesgos y recursos. Se personaliza para adaptarse a los objetivos de cada empresa, traduciendo metas corporativas en metas específicas relacionadas con TI.
2. **Cubrir la Empresa Extremo-a-Extremo:** COBIT 5.0 integra el gobierno y gestión de TI en el contexto corporativo, abarcando todas las funciones y procesos de la empresa. Considera la información y tecnología como activos corporativos y aboga por la inclusión de todos los elementos internos y externos relevantes para el gobierno y gestión de la información y TI.
3. **Aplicar un Marco de Referencia Único Integrado:** COBIT 5 se alinea con otros estándares y marcos de trabajo de TI, convirtiéndose en el marco principal para el gobierno y la gestión de las TI en la empresa.
4. **Hacer Posible un Enfoque Holístico:** COBIT 5.0 adopta un enfoque completo considerando varios componentes interactivos. Define siete categorías de catalizadores (principios, políticas, procesos, estructuras organizativas, cultura, información, servicios y personas) para apoyar la implementación de un sistema global de gobierno y gestión para las TI empresariales. Los habilitadores se dividen en siete categorías las cuales se muestran en la figura 4:

Figura 4

Catalizadores Corporativos de COBIT 5.0.



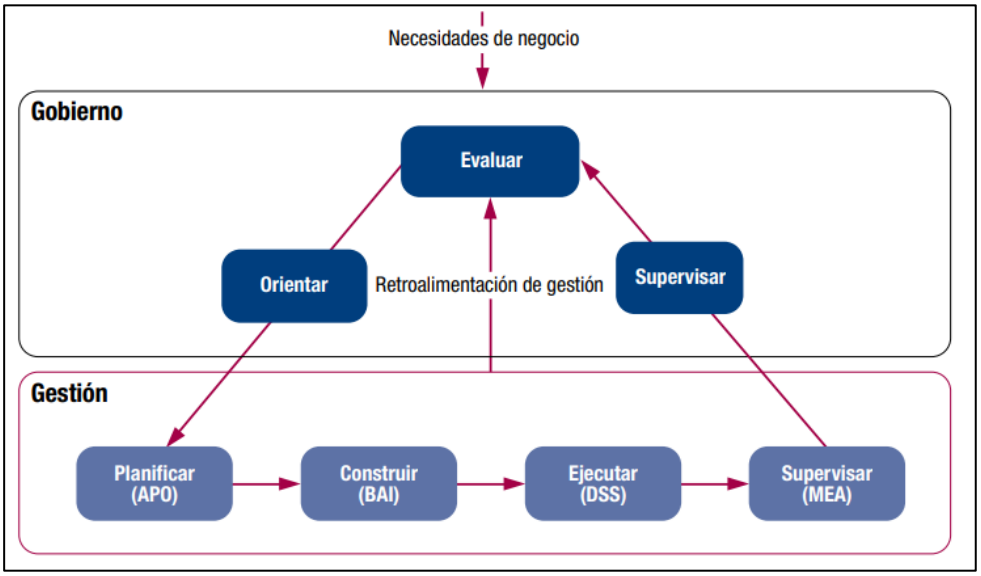
Nota: Catalizadores Corporativos de COBIT 5.0 Los Catalizadores Corporativos de COBIT 5.0, presentados por ISACA en 2012, son componentes clave dentro del marco que facilitan la implementación efectiva de prácticas de gobernanza y gestión, por ISACA, 2012.

5. **Separar el Gobierno de la Gestión:** COBIT 5.0 establece una clara distinción entre el gobierno y la gestión, reconociendo que estas disciplinas implican actividades diferentes, requieren estructuras organizativas distintas y sirven a propósitos diferentes.

   COBIT 5.0 no es obligatorio, pero recomienda que las empresas y organizaciones implementen procesos de gobierno y administración. Esto asegura que las áreas clave estén cubiertas, como se ilustra en la figura 5.

Figura 5

Esquema separación de Gobierno y Gestión.



Nota: Esquema separación de Gobierno y Gestión, ofrece una estructura clara que distingue las actividades de gobernanza de las de gestión dentro de las organizaciones.por ISACA, 2012.

Modelo de procesos de COBIT

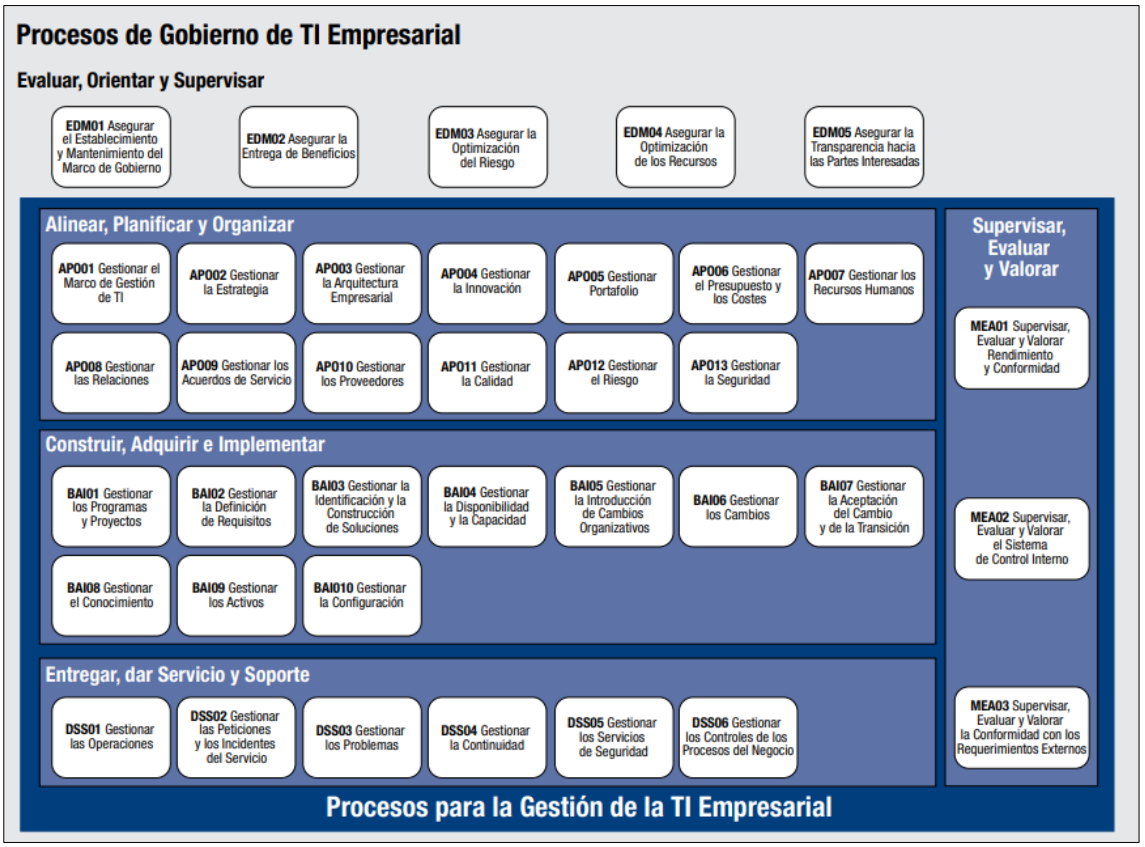
En cada área de actividad de Tecnologías de la Información (TI), existen varios procesos que implican etapas como la planificación, implementación, ejecución y supervisión. Estas etapas son esenciales para resolver cuestiones específicas como calidad y seguridad en los procesos. Estos procesos están agrupados en diferentes dominios según el área de actividad más relevante en el contexto empresarial de TI.

COBIT 5.0 es un modelo de referencia para estos procesos y es la evolución del modelo COBIT

4.1. Además, COBIT 5 incorpora los modelos de procesos de Risk IT y Val IT. En total, COBIT 5 incluye 37 procesos de gobierno y gestión. Todos estos procesos están detalladamente descritos en la guía COBIT 5.0: Procesos Catalizadores, siguiendo el modelo de proceso mencionado anteriormente.

Figura 6

Modelo de Referencia de Procesos de COBIT 5.0



Nota: Modelo de Referencia de Procesos de COBIT 5.0 es un componente central del marco que proporciona una visión estructurada y detallada de los procesos de gobernanza y gestión de TI, por ISACA, 2012.

Definición de la Planeación Estratégica de Tecnologías de la Información (PETI)

La PETI representa un proceso dinámico y continuo en el cual se formulan, implementan y evalúan estrategias relativas a la tecnología de la información en una organización. El objetivo principal de este proceso es alinear las iniciativas tecnológicas con los objetivos y metas generales de la empresa, contribuyendo significativamente a su éxito a largo plazo.

En la PETI, se lleva a cabo un análisis exhaustivo para establecer objetivos tecnológicos que

respalden los objetivos empresariales. Esto implica una evaluación detallada de las necesidades tecnológicas actuales y futuras de la organización, así como la identificación de las oportunidades y desafíos que la tecnología puede presentar en el contexto del mercado y la industria. Además, se identifican los recursos necesarios, tanto humanos como técnicos, y se establecen políticas y procedimientos para garantizar un uso eficaz y eficiente de la tecnología de la información. Este proceso implica también una evaluación constante del desempeño tecnológico, lo que permite realizar ajustes y mejoras continuas para mantener la relevancia y la competitividad en el mercado actual.

En la era digital actual, la PETI se ha vuelto crucial. La competitividad ya no se mide únicamente por la rentabilidad presupuestaria, sino por la capacidad de innovación y diferenciación en un mercado específico. Conceptos como eficiencia, eficacia, calidad, oportunidad, precio, servicio posventa, tecnología y ecología son fundamentales en este contexto (Arias, 2011).

En la competitividad actual, las empresas no solo deben mantenerse, sino también crecer. Esto significa que necesitan encontrar formas nuevas y creativas de hacer negocios, desafiando las ideas tradicionales. Para hacerlo, las empresas utilizan tecnologías avanzadas para manejar la información de manera eficaz. Pero tener tecnología avanzada no es suficiente. Es como tener una herramienta poderosa; es necesario saber cómo usarla de manera inteligente, aquí es donde entra la planeación estratégica (Arias, 2011). En este contexto, el propósito de la Tecnología de la Información es proporcionar recursos claramente definidos para construir, componer e implementar una ventaja competitiva para la empresa (Arias, 2011).

Este enfoque estratégico, especialmente cuando se aplica a tecnologías de información, se centra en la Planeación Estratégica de Tecnologías de Información (PETI). La PETI no es estática, sino dinámica, adaptándose y evolucionando constantemente. Se trata de un proceso continuo que implica la adaptación, innovación y cambio constantes de las estrategias. Estas transformaciones se reflejan en todos los elementos funcionales de la organización, demostrando la interconexión vital entre la estrategia tecnológica y el funcionamiento global de la empresa.

PMBOK (Project Management Body of Knowledge)

PMBOK proporciona una guía completa para la gestión de proyectos, El PMBOK es un documento desarrollado por el Project Management Institute (PMI) que proporciona procesos, prácticas recomendadas, términos y pautas para una gestión de proyectos efectiva incluyendo la identificación y gestión de los alcances, los cronogramas, los costos, la calidad, los riesgos y los recursos involucrados en un proyecto de TIC. Aunque no es una metodología en sí misma, el PMBOK presenta las mejores prácticas y directrices esenciales para supervisar proyectos en todas sus etapas. Esta guía es valiosa tanto para principiantes en el campo de la gestión de proyectos, ya que explica procesos fundamentales que pueden adaptarse a diversas metodologías, como para profesionales experimentados (Rodrigues. N, 2023).

En cada edición, se incorporan innovaciones que responden a las herramientas y necesidades contemporáneas, lo que lo convierte en una herramienta indispensable para los gerentes de proyectos, ofreciendo una orientación completa y sólida para garantizar el éxito en la gestión de proyectos de TIC (Rodrigues. N, 2023).

Lean IT

Lean IT es una extensión y adaptación del modelo de gestión Lean Manufacturing, ampliamente utilizado en procesos industriales, específicamente diseñado para entornos de tecnologías de la información (TI). Su principal objetivo es ayudar a las organizaciones y departamentos de TI a mejorar la entrega de servicios a los clientes al eliminar actividades que no agregan valor. Se centra en la eliminación de desperdicios, la optimización de los flujos de trabajo y la mejora de la eficiencia operativa (Netmind, 2023).

Este enfoque tiene como meta proporcionar valor al cliente mediante la eliminación de actividades innecesarias y mejorando la calidad y velocidad en la entrega de los servicios de TI. Esto se logra gestionando el rendimiento, organizando eficientemente los procesos y fomentando actitudes y comportamientos precisos entre los empleados (García, 2016).

La aplicación de Lean IT abarca todo el dominio de TI, desde los requisitos iniciales hasta el mantenimiento continuo. Además, implica la participación tanto de la alta dirección de la empresa como de todos los trabajadores de la organización. Es importante destacar que Lean

IT se integra de manera complementaria con la mayoría de las guías de buenas prácticas, como ITIL (Information Technology Infrastructure Library) o PRINCE2 (Projects IN Controlled Environments), proporcionando diversas herramientas que permiten analizar y mejorar diversos aspectos de su actuación (Netmind, 2023).

TOGAF (The Open Group Architecture Framework)

TOGAF se centra en optimizar todos los elementos dentro de una empresa para respaldar su estrategia de negocio. La arquitectura empresarial permite una visión global de la empresa, incluyendo procesos, estructura organizativa y tecnologías de la información, lo que facilita el cumplimiento de los objetivos estratégicos, además desempeña un papel fundamental al alinear los objetivos de TI con los objetivos comerciales generales y facilitar la organización de los esfuerzos de TI entre los diferentes departamentos. Este marco ayuda a definir y organizar los requisitos antes de iniciar un proyecto, lo que permite un proceso rápido y con mínimos errores

TOGAF se estructura en dos grupos principales: el contenido fundamental y la orientación ampliada. El contenido fundamental engloba los elementos esenciales y las mejores prácticas de TOGAF, sirviendo como base para el marco. Por otro lado, la orientación ampliada ofrece detalles específicos sobre temas como métodos ágiles, arquitectura empresarial, arquitectura de datos e información, y arquitectura de seguridad. TOGAF puede ser utilizado libremente por cualquier organización, permitiendo su adaptación y personalización según las necesidades específicas. Gracias a esta metodología, las empresas pueden implementar software de manera organizada, enfocándose en la gobernanza y el cumplimiento de sus metas comerciales (Netmind, 2023).

BSC (Balanced Scorecard)

Es un marco de gestión estratégica que se utiliza para medir y gestionar el rendimiento organizativo. Proporciona una estructura para identificar y medir los indicadores clave de rendimiento (KPIs) en diferentes perspectivas, como las finanzas, los clientes, los procesos internos y el aprendizaje y crecimiento. El BSC ayuda a las organizaciones a traducir su estrategia en objetivos medibles y a monitorear su progreso en función de esos indicadores (García. H, 1016).

CAPÍTULO III: METODOLOGÍA

3.1. Tipo de Investigación

En el presente proyecto se aplicará la metodología que combina el enfoque cuantitativo y cualitativo, se utilizarán técnicas estadísticas como el análisis descriptivo, análisis datos recopilados de bibliografías que permitan establecer relaciones cuantitativas entre variables. Se llevará a cabo como técnicas de investigación el análisis de documentos escritos, informes, artículos, registros históricos, entre otros, para extraer información relevante.

Se realizará un estudio descriptivo para para identificar las necesidades y características específicas del sector financiero en Ecuador, sin perder de vista las regulaciones del país y los entornos cambiantes del sistema financiero bancario a nivel nacional, que sin duda está también influenciado por las economías y sectores financieros-bancarios del resto de América y el mundo.

La investigación pondrá énfasis en la exploración documental actualizada a través de la consulta de libros, revistas, periódicos, memorias, anuarios, registros, códices, constituciones, registros web oficiales etc., actualizados y en vigencia.

Por su carácter de documental la investigación se remite a fuentes secundarias que generan los organismos encargados de auditar, monitorear y apoyar a las instituciones bancarias; por lo que se incluye la revisión bibliográfica y toda la tipología de revisiones existentes (revisiones narrativas, revisión de evidencias, meta-análisis, meta-síntesis).

La metodología proporciona una guía o los caminos definidos para aplicar COBIT en el sector financiero del Ecuador, permitiendo una gestión efectiva de TICs y un control de riesgos acorde con las regulaciones y requisitos específicos del sector financiero, esto se realizará comprendiendo el entorno y los requisitos de las instituciones financieras bancarias del país, adaptando y personalizando el marco de referencia COBIT, se identificará los objetivos y controles clave para la gobernanza de Tics evaluando y mejorando el modelo. Se establecerán recomendaciones de monitoreo y auditorias para mantener el modelo vigente en la gobernanza de Tics, con enfoque de mejora continua.

La investigación es de carácter propositiva en base a resultados, conclusiones y recomendaciones que servirán de guía para el desempeño del personal directivo de TI. También se pretende abordar las limitaciones actuales en la gestión de TIC´s y proporcionar un modelo estratégico que promueva su adopción efectiva, demostrando así que las TIC´s representan un beneficio corporativo.

En este proyecto se implementa una metodología mixta, combinando enfoques cuantitativos y cualitativos para ofrecer una comprensión holística de la gobernanza de TICs en el sector financiero de Ecuador. Se utilizan técnicas estadísticas, como el análisis descriptivo, para establecer correlaciones cuantitativas entre variables, directamente alineando esta técnica con el objetivo de identificar patrones claros y medibles dentro del sector financiero que justifiquen la implementación del modelo COBIT.

Se realizarán análisis de documentos tales como informes escritos, artículos y registros históricos, lo que permitirá extraer información crítica que respalda la necesidad de un modelo de gobernanza efectivo. Este enfoque descriptivo es crucial para comprender las condiciones específicas del sector financiero en Ecuador, respetando las regulaciones nacionales y adaptándose a los dinámicos cambios del mercado global.

Justificación de Métodos y Procedimientos

- **Análisis Descriptivo**: Utilizado para cuantificar y describir características fundamentales del sector financiero. Este método es esencial para evaluar la efectividad actual de las estrategias de gobernanza de TICs y determinar áreas clave de mejora.
- **Estudio Documental**: Facilita una revisión profunda de las tendencias contemporáneas y las prácticas regulatorias a través de fuentes secundarias. Esto es fundamental para asegurar que el modelo de planeación estratégica propuesto esté bien informado y contextualizado.
- **Consultas Documentales:** El acceso a una variedad de documentos actualizados permite integrar perspectivas diversificadas y robustecer la propuesta de modelo con evidencia concreta y relevante.

Diagrama de Flujo de la Metodología de Investigación	**Inicio:** Comienza el proceso de investigación.
	Recolección de Datos: Recopilación de datos de bibliografías, documentos, informes, artículos, registros históricos, etc.
	Análisis Descriptivo y Documental: Utilización de técnicas estadísticas para análisis descriptivo. Análisis de documentos escritos y otros materiales para extraer información relevante.
	Identificación de Necesidades: Estudio descriptivo para identificar las necesidades y características específicas del sector financiero en Ecuador.
	Aplicación del Modelo COBIT: Implementación del modelo COBIT en el contexto del estudio.
	Personalización del Modelo: Adaptación del modelo COBIT a las necesidades específicas del sector financiero en Ecuador.
	Implementación de Controles: Establecimiento de controles de riesgos y procedimientos de evaluación continua.
	Evaluación y Auditorías: Monitoreo y auditorías para evaluar la eficacia del modelo y realizar mejoras continuas.

Resultados esperados:

- Propuesta de modelo de planeación estratégica de Tics-Gobernanza con COBIT para empresas del sector financiero bancario en el Ecuador.
- Lineamientos del sector financiero bancario en Ecuador, incluyendo las regulaciones y marcos legales relacionados con la gobernanza de TIC´s, para adaptar el modelo a los requisitos específicos del contexto local junto a la implementación del respectivo road map.
- Aplicar COBIT con sus mejores prácticas reconocidas a nivel internacional como marco de gobernanza y gestión de TIC´s.
- Procesos generales para diseñar y aplicar un modelo de planeación estratégica de Tics-Gobernanza con COBIT adaptado a entornos competitivos, exigentes y cambiantes con tecnologías que aplican inteligencia artificial.
- Mecanismos para controles de riesgos, procedimientos, evaluación continua e indicadores o KPI´s alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector financiero bancario en Ecuador.

3.2. Diseño de Investigación

1. Identificar el entorno del sector financiero bancario en Ecuador, incluyendo las

regulaciones y marcos legales relacionados con la gobernanza con COBIT, para adaptar el modelo a los requisitos específicos del contexto local.

Para alcanzar el primer objetivo específico de este proyecto de titulación, se llevará a cabo una revisión documental exhaustiva del entorno del sector financiero en Ecuador, con un enfoque en las regulaciones y marcos legales relacionados con la gobernanza basada en COBIT. Esto implicará un análisis detallado de la literatura existente sobre prácticas bancarias en Ecuador, incluyendo leyes, regulaciones, normativas y estándares asociados a la gobernanza de las tecnologías de la información y comunicación (TIC) en el ámbito bancario.

Además, se realizará un análisis comparativo entre las regulaciones y prácticas internacionales, como las mejores prácticas de COBIT a nivel global, y las regulaciones y prácticas locales en Ecuador. El objetivo principal es identificar las brechas y diferencias clave entre estos dos contextos normativos.

Para obtener una comprensión más precisa del marco regulatorio y legal en el país, se examinarán documentos oficiales publicados por los reguladores financieros y gubernamentales en Ecuador, así como las leyes y reglamentos que impactan a las instituciones bancarias.

2. Determinar los procesos de COBIT a implementarse como marco de gobernanza y gestión de TIC´s junto a la implementación del respectivo road map.

Para cumplir con el segundo objetivo específico se adquirirá un profundo conocimiento de COBIT a través de un estudio descriptivo, tomando sus principios, objetivos y procesos clave que conforman un marco de referencia. Además, se llevará a cabo la revisión exhaustiva de la documentación disponible sobre COBIT. Esto incluye los estándares y guías oficiales proporcionados por ISACA (la organización detrás de COBIT), así como cualquier literatura relevante y casos de estudio que aborden la implementación de COBIT en el sector financiero y en entornos similares.

Es importante identificar los procesos de COBIT que son relevantes y necesarios para la gobernanza y gestión de TIC en el contexto específico de las instituciones financieras

en Ecuador. Esto puede requerir la adaptación y personalización de los procesos de COBIT para satisfacer las necesidades y requisitos locales.

Adicionalmente, establecerán los objetivos para cada proceso de COBIT que se planea implementar. Estos objetivos estarán alineados con las metas estratégicas de las instituciones bancarias y sus necesidades específicas en términos de gobernanza de TIC. Además, se llevará a cabo el diseño un road map detallado que describa la secuencia y los pasos necesarios para implementar los procesos de COBIT identificados. Esto incluye la asignación de recursos, plazos, responsabilidades y cualquier otro elemento relevante para la implementación exitosa.

3. Determinar las buenas práctica y estándares generales para diseñar y aplicar un modelo de planeación estratégica de Tics-Gobernanza con COBIT adaptado a entornos competitivos, exigentes y cambiantes.

   Para cumplir con el tercer objetivo específico se realizará una revisión exhaustiva de la literatura especializada en el campo de la gobernanza de TIC y COBIT, fuentes confiables que aborden buenas prácticas y estándares internacionales en la implementación de COBIT en entornos similares, especialmente en el sector financiero. Se buscará un caso de estudio relacionados con la implementación exitosa de COBIT en instituciones financieras de otros países o regiones que enfrenten desafíos y dinámicas similares.

   Se plantearán e identificarán las buenas prácticas y estándares clave que sean relevantes para la gobernanza de TIC en entornos competitivos y cambiantes. Estos pueden incluir enfoques de gestión de riesgos, estrategias de adaptación tecnológica y métodos para la toma de decisiones basadas en datos, entre otros. Además, se adaptarán a los requisitos y particularidades del sector financiero bancario en Ecuador para abordar las necesidades locales y los desafíos específicos que enfrentan las instituciones bancarias en el país.

   En base a las buenas prácticas y estándares identificados y adaptados, se diseñará el modelo de planeación estratégica de Tics-Gobernanza con COBIT que sea adecuado para entornos competitivos y cambiantes el cual estará alineado con los objetivos

estratégicos de las instituciones bancarias en Ecuador.

4. Proponer mecanismos para control de riesgos, procedimientos, evaluación continua e indicadores o KPI alineados con las mejores prácticas de COBIT y adaptados a los requisitos específicos del sector financiero bancario en Ecuador.

Para cumplir con el cuarto objetivo se identificarán los riesgos específicos asociados al sector financiero bancario en Ecuador, esto puede incluir riesgos relacionados con la seguridad de datos, ciberseguridad, continuidad del negocio y cumplimiento de regulaciones locales, también se examinará las mejores prácticas de COBIT relacionadas con la gestión de riesgos, procedimientos y evaluación continua debido a que proporciona un marco sólido para la gestión de riesgos y la toma de decisiones basadas en datos.

Se adaptarán las mejores prácticas de COBIT para satisfacer los requisitos y regulaciones específicas del sector financiero bancario en Ecuador, procurando que las recomendaciones sean relevantes y aplicables a este entorno. Además, se diseñará procedimientos y controles específicos que aborden los riesgos identificados. Esto puede incluir políticas de seguridad de datos, protocolos de respuesta a incidentes y procedimientos de cumplimiento normativo.

Finalmente se definirán los indicadores clave de rendimiento (KPI) que permitan evaluar la efectividad de los procedimientos y controles implementados, los cuales estarán alineados con las metas estratégicas de las instituciones bancarias y proporcionar una medida cuantitativa de su desempeño en la gestión de riesgos, además establecerá un modelo de proceso de evaluación continua para monitorear la efectividad de los mecanismos de control de riesgos y procedimientos.

3.3. Unidades de Estudio

El sector financiero bancario, tanto a nivel mundial como nacional, desempeña un papel crucial en la generación de empleos y el aumento de la productividad económica. Los sistemas bancarios y los mercados de capital sólidos son fundamentales para facilitar el flujo eficiente de fondos hacia inversiones productivas, respaldar la recaudación de capital de inversión por parte de los Gobiernos, mantener redes de seguridad financiera y garantizar la seguridad en las transacciones financieras transfronterizas (Sector Financiero, 2021).

Además, la banca y la tecnología se han vuelto inseparables en la actualidad, ya que la actividad bancaria depende en gran medida de la tecnología para ofrecer servicios eficientes y de calidad a los usuarios finales. En este contexto, la gobernanza IT con COBIT, como marco formal, desempeña un papel esencial al garantizar que las inversiones en tecnología de la información estén alineadas con los objetivos empresariales (Danby, 2023).

3.4. Técnicas e instrumentos de recolección de datos

En el marco de la presente investigación, se ha seleccionado la observación como el método primordial de recolección de datos. Esta elección se fundamenta en la naturaleza directa del trabajo en un entorno bancario, donde se busca emplear técnicas de observación directa para analizar las prácticas vigentes de gobernanza de TIC, haciendo hincapié en la ejecución de la planeación estratégica.

La observación directa permitirá una inmersión práctica en el entorno, posibilitando una comprensión detallada de la implementación de las estrategias de gobernanza de TIC. Este enfoque resulta particularmente pertinente en un contexto financiero, donde la ejecución efectiva de la planificación estratégica es esencial para el éxito operativo.

Adicionalmente, se llevará a cabo un análisis documental, una práctica complementaria que involucra la revisión de documentos relevantes, como informes internos y políticas organizacionales. Esta técnica se empleará para consolidar y enriquecer la información recopilada durante la observación, proporcionando una visión más integral de las prácticas de gobernanza de TIC en el sector bancario.

Al combinar la observación directa con el análisis documental, se busca obtener una perspectiva holística y en profundidad de la gobernanza de TIC en el entorno específico de las entidades financieras. Este enfoque metodológico robusto permitirá una interpretación más completa de las dinámicas y procesos relacionados con la planificación estratégica en el sector bancario ecuatoriano.

3.5. Técnica de Análisis de Datos

Instrumentos de Recolección de Datos para la Tesis:

En el marco de un enfoque cualitativo, la aplicación de la técnica documental se presenta como una herramienta esencial para la selección de información proveniente de documentos, libros y revistas científicas. Este método se erige como un pilar fundamental que habilitará la recopilación de datos detallados, necesarios para el desarrollo integral de la solución propuesta en la investigación (Echaverría, 1999).

La técnica documental posibilita acceder a una amplia base de conocimientos, aprovechando la vasta información contenida en documentos especializados, libros relevantes y revistas científicas. Esto enriquecerá la investigación al permitir la revisión y síntesis de antecedentes clave. Al extraer información detallada mediante esta técnica, se establece un fundamento sólido para el desarrollo de la solución propuesta. La profundidad y la calidad de los datos obtenidos a través de documentos respaldarán la construcción de un marco conceptual robusto. La técnica documental facilitará la determinación precisa del modelo de gobernanza con COBIT. Al analizar documentos especializados en esta área, se obtendrá una comprensión clara de los principios y prácticas que sustentan la aplicación de COBIT en el contexto específico de la investigación.

ANALISIS Y CONTEXTO DEL SECTOR FINANCIERO BANCARIO EN ECUADOR

Establecimientos Bancarios

En el contexto ecuatoriano, los establecimientos bancarios se definen como instituciones financieras cuya función principal es la captación de recursos en cuentas corrientes y otros depósitos, con el objetivo principal de llevar a cabo operaciones activas de crédito. En el ámbito de los bancos comerciales, se refiere a entidades que reciben fondos en depósito general para utilizarlos, junto con su propio capital, en préstamos y en la adquisición o descuento de pagarés, giros o letras de cambio. Por otro lado, los bancos hipotecarios en Ecuador se caracterizan por proporcionar préstamos respaldados por bienes raíces, los cuales deben ser cubiertos mediante pagos periódicos, y tienen la facultad de emitir cédulas de inversión. Estas funciones buscan contextualizar las actividades financieras dentro de la normativa y prácticas específicas del sistema bancario en el país (Asobanca, 2022).

Situación actual de las TIC en el sector Bancario

Internet ha ocasionado transformaciones significativas en el ámbito bancario. La incorporación de Tecnologías de la Información y Comunicación (TIC) permite a las entidades competir en un mercado cada vez más saturado, ofreciendo una gama más extensa y sofisticada de productos. Sin embargo, también plantea desafíos, especialmente en cuanto a seguridad y la gestión cada vez más compleja de la información.

En el ámbito de la gestión al cliente, las instituciones financieras están enfocadas en ampliar sus servicios en línea, lo que conlleva inevitablemente aspectos tecnológicos como la seguridad y el manejo cada vez mayor de datos. Un estudio de la Asociación Europea de Gestión Financiera (EFMA) destaca la importancia significativa de la atención al cliente, vinculando la excelencia en este ámbito con la digitalización de los servicios. Este enfoque busca dirigir estrategias y operaciones hacia el cliente, empleando Tecnologías de la Información para mejorar la cercanía y agilizar los tiempos de respuesta mediante optimizaciones operativas y mayor automatización (Cabero, 2022).

En relación con la inversión en tecnologías, las instituciones bancarias reconocen la vital importancia de las TIC para potenciar sus operaciones. Aunque algunas ya cuentan con infraestructuras sólidas para gestionar los cambios tecnológicos, otras enfrentan limitaciones en sus actuales infraestructuras tecnológicas. En este contexto, la Gobernanza de TIC se revela como un elemento fundamental para alinear los objetivos institucionales con la inversión en tecnologías de la información y comunicación. Según el estudio de la EFMA, los bancos buscan incrementar sus transacciones mediante la creación de entornos donde los clientes puedan acceder a una variedad más amplia de productos y servicios a través de diversos canales.

Dentro de los objetivos de la gobernanza, la seguridad en el ámbito bancario se posiciona como un aspecto crucial. A pesar de las medidas implementadas, como la identificación del cliente y la encriptación de la información, persisten desafíos notables. Los ciberataques, como el phishing a través del correo electrónico, continúan representando una amenaza, según revela un estudio de la Asociación de Internautas. Aunque se establecen medidas de seguridad, la falta de fiabilidad en los mecanismos de verificación de la identidad de los usuarios sigue siendo un obstáculo significativo (Cabero, 2022).

Superintendencia de bancos

En Ecuador, la Superintendencia de Bancos (SB) tiene la responsabilidad de supervisar y controlar las actividades de entidades financieras y de seguridad social para proteger los intereses de la ciudadanía, garantizando la seguridad, estabilidad y transparencia de estas instituciones (Superintendencia de Bancos, 2023).

La SB emitió el plan estratégico de tecnologías de la información y comunicación (PETIC) bajo la dirección de la Coordinación General de Tecnologías de Información y Comunicación (CGTIC), específicamente la Dirección de Gobernanza de TI e Innovación.

La Resolución No. SB-2019-1025 del 27 de septiembre de 2019 aprobó el Plan Estratégico Institucional (PEI) de la SB para el período 2019-2024. El PEI, modificado en 2020, orienta la consecución de objetivos, dando lugar al desarrollo del PETIC para gestionar activos informáticos y soluciones digitales. A pesar de restricciones presupuestarias, el PETIC se alinea con el PEI y cumple con normativas. La CGTIC supervisa entidades con un enfoque resiliente y basado en riesgos (Superintendencia de Bancos, 2021).

CAPÍTULO IV: PRESENTACIÓN DE LA PROPUESTA

ALINEACIÓN CON LOS OBJETIVOS DEL PLAN ESTRATÉGICO

Gestión Tecnológica para la Supervisión Basada en Riesgos

Para la consecución de la Gestión Tecnológica para la Supervisión Basada en Riesgos, se propone establecer un portafolio anual de TIC alineado con el PEI 2019-2024 y sus reformas, Tabla 1 (Superintendencia de Bancos, 2021)..

Tabla 1

Objetivos de Gobierno y Gestión COBIT alineados a la Estrategia Institucional.

Pilar Estratégico	**Objetivo Estratégico Institucional / Objetivos Estratégicos de Tecnologías de Información y Comunicación**	**Objetivo de Gobernabllidad y Gestión**
Preservar la estabilidad de los sectores público y privado del sistema financiero y del sistema de seguridad social.	-Apoyar la automatización de los procesos gobernantes, sustantivos y adjetivos.	EDM01: Asegurar el establecimiento y el Mantenimiento del marco de gobierno. EDM03: Asegurar la optimización del riesgo APO12: Gestionar el riesgo APO13: Gestionar la seguridad

		BAI10: Gestionar la configuración DSS04: Gestionar la continuidad
Incrementar la eficiencia y efectividad del modelo de supervisión y control preventivo, integral, prospectivo y suficiente basado en riesgos	-Apoyar la automatización de los procesos gobernantes, sustantivos y de apoyo. -Garantizar la seguridad de la información, a través de mecanismos de protección de datos. -Mantener la plataforma de TI actualizada para la incorporación de nuevas soluciones tecnológicas y correcta mantención de sistemas operativos.	EDM01: Asegurar el establecimiento y el Mantenimiento del marco de gobierno. EDM04: Asegurar la optimización de los recursos AP002: Gestionar la estrategia. APOOS: Gestionar el portafolio APO06: Gestionar el presupuesto y los costes APO07: Gestionar los recursos humanos. AP009: Gestionar los acuerdos de servicio. APO11: Gestionar la calidad BAI02: Gestionar la definición de requisitos BAI03: Gestionar la identificación y construcción de soluciones BAI04: Gestionar la disponibilidad y capacidad BAI06: Gestionar los cambios de TI BAI07: Gestionar la aceptación y la transición de los cambios de TI BAI08: Gestionar el conocimiento 8AI09: Gestionar los activos BAI11: Gestionar los proyectos DSS01: Gestionar las operaciones DSS02: Gestionar las peticiones y los incidentes de servicio DSS03: Gestionar los problemas. DSS04: Gestionar la continuidad. MEA01: Gestionar la monitorización del desempeño y la conformidad

Propender a la eficacia y a la innovación regulatoria de los sistemas controlados	-Apoyar la automatización de los procesos gobernantes, sustantivos y de apoyo.	EDM01: Asegurar el establecimiento y el Mantenimiento del marco de gobierno. EDM03: Asegurar la optimización del riesgo EDM04: Asegurar la optimización de los recursos APO02: Gestionar la estrategia. APO05: Gestionar el portafolio APO06: Gestionar el presupuesto y los costes APO07: Gestionar los recursos humanos. APO11: Gestionar la calidad APO12: Gestionar el riesgo APO13: Gestionar la seguridad BAI02: Gestionar la definición de requisitos BAI03: Gestionar la identificación y construcción de soluciones. BAI08: Gestionar el conocimiento. BAI10: Gestionar la configuración. BAI11: Gestionar los proyectos. DSS04: Gestionar la continuidad.
Promover la migración hacia un sistema financiero inclusivo, basado en la innovación, protección al consumidor y la educación financiera	-Apoyar la automatización de los procesos gobernantes, sustantivos y de apoyo. -Garantizar la seguridad de la información, a través de mecanismos de protección de datos.	APO02: Gestionar la estrategia APO06: Gestionar el presupuesto y los costes AP007: Gestionar los recursos humanos BAI08: Gestionar el conocimiento BAI09: Gestionar los activos
Re-institucionalizar la Superintendencia de Bancos mediante el fortalecimiento del juicio experto, capacitación innovativa y el ejercicio pleno de su autonomía	-Apoyar la automatización de los procesos gobernantes, sustantivos y de apoyo. - Mantener la plataforma de TI actualizada para la incorporación de nuevas soluciones tecnológicas y	AP006: Gestionar el presupuesto y los costes AP007: Gestionar los recursos humanos APO11: Gestionar la calidad BAI08: Gestionar el conocimiento BAI09: Gestionar los

	correcta mantención de sistemas.	activos MEA01: Gestionar la monitorización del desempeño y la conformidad

Cuando los procesos de TIC siguen los Objetivos de Gobierno y Gestión de COBIT 2019, se crea una guía para adoptar buenas prácticas en la gestión de la tecnología. Estas prácticas se basan en objetivos específicos, algunos de los cuales son responsabilidad directa o parcial de la CGTIC en las organizaciones. En ciertos casos, se necesitan definiciones organizacionales a las que la Tecnología de la Información debe ajustarse para su correcta gestión, esta información se presenta en la Tabla 2 (Superintendencia de Bancos, 2021).

Tabla 2

Objetivos de Gobierno y Gestión COBIT para procesos de TIC (arriba párrafo adiciendo que ya se va a nfocar)

Objetivos COBIT		**Objetivos TIC SB**	**Objetivos de Gobierno / Gestión**
Objetivos de Gobierno	Evaluar, dirigir y monitorizar	Gobierno de TI	EDM01: Asegurar el establecimiento y el Mantenimiento del marco de gobierno
		Seguridad Informática	EDM03: Asegurar la optimización del riesgo
		Gobierno de TI	EDM04: Asegurar la optimización de los recursos
Objetivos de Gestión	Alinear, Planificar y Organizar	Gobierno de TI	AP002: Gestionar la estrategia
		Portafolio de TIC	APOO5: Gestionar el portafolio
		Portafolio de TIC	APO06: Gestionar el presupuesto y los costes
		Disponibilidad y capacidad	APO07: Gestionar los recursos humanos
		Acuerdos de Niveles de Servicio	APO09: Gestionar los acuerdos de servicio
		Construcción de soluciones	APO11: Gestionar la calidad
		Seguridad Informática	APO12: Gestionar el riesgo
		Seguridad Informática	APO13: Gestionar la seguridad

	Construir, adquirir e implementar	Construcción de soluciones	BAI02: Gestionar la definición de requisitos
		Construcción de soluciones	BAI03: Gestionar la identificación y construcción de soluciones
		Disponibilidad y capacidad	BAI04: Gestionar la disponibilidad y capacidad
		Cambios y configuración	BAI06: Gestionar los cambios de TI
		Cambios y configuración	BAI07: Gestionar la aceptación y la transición de los cambios de TI
		Cambios y configuración	BAI08: Gestionar el conocimiento
		Seguridad Informática	BAI09: Gestionar los activos
		Cambios y configuración	BAI10: Gestionar la configuración
		Portafolio de TIC	BAI11: Gestionar los proyectos
	Entregar, dar servicios y soporte	Operaciones	DSS01: Gestionar las operaciones
		Requisitos Incidentes y problemas	DSS02: Gestionar las peticiones y los incidentes de servicio
		Requisitos Incidentes y problemas	DSS03: Gestionar los problemas
		Continuidad	DSS04: Gestionar la continuidad
	Monitorizar, evaluar y valorar	Acuerdos de Niveles de Servicio	MEA01: Gestionar la monitorización del desempeño y la conformidad

DIRECCONAMIENTO ESTRATÉGICO DE TIC

La misión del direccionamiento estratégico de TIC es gestionar, asesorar y coordinar los recursos tecnológicos de la entidad mediante soluciones innovadoras, en concordancia con las políticas de seguridad informática y aseguramiento de la calidad. El objetivo es alinear la gestión tecnológica con el plan estratégico institucional y la normativa legal vigente.

La visión es alcanzar reconocimiento institucionalmente por la calidad de los servicios tecnológicos innovadores, alineados a los pilares estratégicos, que contribuyan a los procesos gobernantes, sustantivos y adjetivos.

Objetivos Estratégicos de Tecnologías de la Información y Comunicación

Para lograr una supervisión adecuada y eficaz, se busca la alineación estratégica tecnológica

con las necesidades de la Superintendencia de Bancos, conforme a los lineamientos del Plan Estratégico Institucional y la Arquitectura Empresarial (Superintendencia de Bancos, 2021). Estos objetivos se resumen en:

1. **Apoyar la automatización de los procesos gobernantes, sustantivos y adjetivos**: Busca respaldar la automatización de los procesos esenciales y relacionados con la gestión y gobierno, contribuyendo a la eficiencia operativa.

2. **Garantizar la seguridad de la información mediante mecanismos de protección de datos**: Orientado a asegurar la integridad y confidencialidad de la información mediante la implementación de medidas de seguridad y protección de datos.

3. **Mantener la plataforma de TI actualizada para incorporar nuevas soluciones tecnológicas y garantizar la correcta mantención de sistemas operativos**: Busca asegurar la modernización constante de la infraestructura tecnológica para incorporar innovaciones y garantizar el adecuado funcionamiento de los sistemas operativos.

Entendimiento Estratégico

El Entendimiento Estratégico se define como la capacidad para vincular los objetivos estratégicos institucionales con los objetivos estratégicos tecnológicos. Este proceso ofrece a la Coordinación General de Tecnologías de Información y Comunicación la orientación necesaria para utilizar la tecnología como un agente de transformación organizacional.

Este entendimiento implica establecer y comprender los procesos que tienen lugar en el entorno organizacional, así como las interacciones y servicios del sector con diversos grupos de interés. El propósito final es proporcionar a la coordinación los elementos esenciales para identificar oportunidades y desafíos de Tecnologías de la Información que contribuyan al logro de la estrategia institucional.

Además, la alineación de los objetivos estratégicos de TIC con las rupturas estratégicas posibilita focalizar de manera técnica la gestión y los proyectos tecnológicos. Esto permite abordar y priorizar tanto las necesidades institucionales como los problemas fundamentales que enfrenta en la actualidad, todo ello guiado por una visión de largo plazo.

El logro de los objetivos del Plan Estratégico de Tecnologías de la Información y Comunicación se fundamenta en aspectos generales, tales como la reestructuración y caracterización de procesos alineados con la cadena de valor, respaldada por marcos de referencia como COBIT e ITIL.

Modelo de Planeación y lineamientos de Plan Estratégico

El modelo de planeación incluye los lineamientos que guían la definición del Plan Estratégico Tecnológico, tabla 3.

Tabla 3

Modelo de planeación incluye los lineamientos que guían la definición del Plan Estratégico Tecnológico (Superintendencia de Bancos, 2021).

Componente del Modelo	**Producto**	**Actividad**
Gobierno de TI	Plan Estratégico de TI	Proceso de Gobierno y de Gestión
		Políticas, Normas y Procedimientos
		Marco de Gobierno de TI
		Procesos de TI establecidos

EJEMPLO DE APLICACIÓN DE BUENA PRÁCTICA APO13 EN LA PLANEACIÓN ESTRATÉGICA TIC-GOBERNANZA PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL BANCO PICHINCHA.

La evolución constante de las tecnologías y la creciente integración de servicios digitales en la vida diaria han revolucionado la forma en que las empresas operan, ofreciendo numerosas ventajas y comodidades a los usuarios. No obstante, este avance tecnológico también ha modificado significativamente el panorama de riesgos tradicional, presentando nuevos desafíos para las organizaciones. Un aspecto crítico de esta transformación es el aumento de actividades

delictivas en el ámbito digital, lo que pone de relieve la urgente necesidad de reformar y fortalecer los modelos de planeación estratégica en la seguridad de la información.

Estos programas deben no solo abordar los riesgos emergentes, sino también alinearse estrechamente con los objetivos de negocio. En este sentido, es vital adoptar un modelo estandarizado para la gestión de la seguridad de la información, como COBIT, que ofrezca un enfoque estructurado y adaptable a cualquier organización. La adopción de tal modelo es especialmente crucial en el sector bancario, donde la seguridad de la información es fundamental para proteger los activos de los clientes y mantener la confianza en el sistema financiero. Asimismo, la alineación de las prácticas de seguridad con un marco como COBIT asegura que las instituciones bancarias no solo estén preparadas para enfrentar los desafíos actuales, sino también para adaptarse con agilidad a las dinámicas cambiantes que conlleva la globalización.

En este capítulo, se presentará un ejemplo práctico de planeación estratégica TIC-Gobernanza en el Banco Pichincha, utilizando la metodología de COBIT y centrándose particularmente en la seguridad de la información. Se aplicará la buena práctica APO13 de COBIT y se examinarán las directrices impuestas por la Superintendencia de Bancos de Ecuador. Este enfoque asegura no solo el cumplimiento de las normativas locales, sino también el fortalecimiento de la estructura de seguridad de la información del banco.

Procesos definidos por COBIT impuestos por la Superintendencia de Bancos para seguridad de la información.

La implementación de las prácticas de COBIT en el contexto de la seguridad de la información y la planificación estratégica de TI en el Banco Pichincha implicaría la adopción de los siguientes procesos clave:

- **APO13 - Gestionar la Seguridad**: Esta práctica es esencial para desarrollar y mantener un marco de seguridad de la información robusto y eficaz que proteja contra amenazas y cumpla con las directrices de la SB. APO13 asegura que la seguridad de la información se gestione como un proceso integral, abarcando desde la identificación de riesgos hasta la implementación de controles de seguridad adecuados.

- **DSS05 - Gestionar la Seguridad de los Servicios de TI**: Esta práctica se enfoca en la protección efectiva de los servicios de TI, garantizando que estén alineados con los requisitos de seguridad y conformidad establecidos por la SB.
- **APO12 - Gestionar el Riesgo**: Esta práctica es fundamental para identificar y gestionar proactivamente los riesgos asociados con la seguridad de la información.
- **DSS01 - Gestionar las Operaciones de TI**: Esta práctica asegura que las operaciones diarias de TI del banco estén en concordancia con las políticas de seguridad y los estándares regulatorios.
- **MEA03 - Asegurar la Conformidad con Políticas y Normas Externas**: Implica una revisión y evaluación regulares de la conformidad de las operaciones de TI con las normativas y políticas externas, incluyendo las especificadas por la Superintendencia.
- **DSS04 - Gestionar la Continuidad del Negocio**: Establece un plan de continuidad del negocio y recuperación de desastres en línea con los requisitos de la resolución, garantizando así la resiliencia operativa del banco.

Como parte de los objetivos de este trabajo de titulación, se presentará un ejemplo práctico de aplicación de la práctica COBIT APO13 en el área de seguridad de la información. Este ejemplo servirá para ilustrar cómo las instituciones financieras como el Banco Pichincha pueden integrar efectivamente las prácticas de COBIT para mejorar su seguridad de la información, alineándose así con los estándares de la industria y los requisitos regulatorios.

En octubre de 2021, el Banco Pichincha experimentó un incidente significativo de seguridad en línea, que afectó sus sistemas electrónicos y, consecuentemente, a sus usuarios. Este incidente, atribuido a un hackeo, subrayó la importancia crítica de robustecer las medidas de seguridad en el sector bancario, especialmente en lo que respecta a la protección de datos del cliente y la seguridad en las transacciones en línea. En respuesta, el Banco Pichincha anunció la implementación de medidas de seguridad reforzadas y la intervención de una auditoría por parte de la Superintendencia de Bancos, aunque los resultados específicos de estas acciones no se han divulgado públicamente hasta la fecha.

Este incidente resalta la necesidad continua de evaluación y mejora de la seguridad de la información, alineándose con prácticas recomendadas y estándares como los proporcionados por COBIT para la gestión de riesgos de seguridad. Las instituciones financieras deben enfocarse en la identificación proactiva de riesgos, estableciendo controles específicos y

adoptando tecnologías avanzadas de seguridad para prevenir ataques cibernéticos, filtraciones de datos y fraudes internos. Además, la capacitación y concienciación sobre la seguridad de la información se vuelve imperativa para todos los niveles de la organización, asegurando que se mantengan prácticas seguras y se mejore la respuesta a incidentes.

Tabla 4

Aplicación Teórica de APO13 - Gestionar la Seguridad en el Banco Pichincha

Evaluación Inicial de la Seguridad de la Información	Análisis de Necesidades de Seguridad	• Protección de Datos del Cliente • Seguridad en Transacciones en Línea • Cumplimiento Normativo
	Supuestos de Infraestructura de TI	• Sistemas de Banca en Línea y Móvil • Bases de Datos de Clientes • Redes Internas y Externas
Desarrollo de un Marco de Seguridad de la Información en el Banco Pichincha	Políticas de Seguridad	• Fundamentos • Alcance de la Política • Roles y Responsabilidades
	Procedimientos y Controles	• Establecimiento de Controles • Controles Específicos
Gestión de Riesgos de Seguridad	Identificación de Riesgos	• Ataques Cibernéticos • Filtraciones de Datos • Fraudes Internos
	Plan de Mitigación de Riesgos	• Adopción de Tecnologías de Seguridad Avanzadas • Protocolos de Respuesta a Incidentes • Capacitación y Concienciación • Auditorías y Revisiones Continuas
Aplicación del Plan de Mitigación de Riesgos	Gestión Proactiva de Incidentes Anteriores	• Gestión Proactiva de Incidentes Anteriores • Mejoras Tecnológicas y Educación Continua • Auditorías Enfocadas en Experiencias Previas
	Evaluación de Necesidades y	• Diagnóstico de Competencias • Identificación de Áreas Críticas

Capacitación y concienciación en seguridad de la información	Análisis de Público Objetivo	
	Diseño del Programa de Capacitación	• Contenidos Específicos • Metodologías Diversificadas
	Implementación y Participación Activa	• Planificación de Sesiones • Inclusión de Expertos
	Evaluación Continua y Mejora	• Pruebas de Conocimiento • Simulacros de Seguridad
	Mantenimiento de la Concienciación	• Comunicación Regular • Embajadores de Seguridad

Introducción

- **Propósito:** Implementar APO13 de COBIT en el Banco Pichincha para fortalecer la gestión de la seguridad de la información.
- **Contexto:** Consideración de la importancia de la seguridad de la información en el sector bancario y el enfoque proactivo que se requiere para gestionar los riesgos digitales.

Evaluación Inicial de la Seguridad de la Información

La evaluación inicial de la seguridad en el Banco Pichincha debe centrarse en la protección de datos del cliente, seguridad en transacciones en línea, y el cumplimiento normativo. Esto implica un análisis riguroso de la infraestructura de TI existente, incluyendo sistemas de banca en línea y móvil, bases de datos de clientes, y redes internas y externas.

Análisis de Necesidades de Seguridad

- **Protección de Datos del Cliente**: En el sector bancario, la protección de datos del cliente es primordial. El Banco Pichincha, como una de las instituciones financieras líderes en Ecuador, maneja una gran cantidad de información sensible. Es fundamental implementar políticas y prácticas robustas de seguridad de datos para prevenir amenazas como el fraude y la usurpación de identidad, así como para cumplir con las regulaciones de protección de datos.

- **Seguridad en Transacciones en Línea**: Dada la prevalencia de servicios bancarios en línea y móviles, asegurar las transacciones digitales es crucial. Esto incluye la implementación de autenticación fuerte, cifrado y otras medidas de seguridad para proteger contra el phishing, el spoofing y otros tipos de ataques cibernéticos.
- **Cumplimiento Normativo**: La regulación financiera es un aspecto crítico para los bancos. En este caso, el Banco Pichincha debe adherirse a las normativas locales e internacionales relacionadas con la ciberseguridad y la protección de datos. Esto requiere una continua evaluación y actualización de las prácticas de seguridad para garantizar el cumplimiento.

Supuestos de Infraestructura de TI

- **Sistemas de Banca en Línea y Móvil**: La infraestructura de TI del Banco Pichincha incluye sistemas avanzados para la banca en línea y móvil. Estos sistemas necesitan estar protegidos con las últimas tecnologías de seguridad para prevenir accesos no autorizados y garantizar la integridad de las transacciones.
- **Bases de Datos de Clientes**: Las bases de datos que almacenan información personal y financiera de los clientes deben estar seguras contra brechas y fugas de datos. Esto implica el uso de soluciones de seguridad de bases de datos, encriptación de datos y controles de acceso estrictos.
- **Redes Internas y Externas**: La protección de las redes del banco contra intrusiones y ataques cibernéticos es vital. Esto incluye la implementación de firewalls, sistemas de detección y prevención de intrusiones, y la segmentación de redes para controlar el flujo de datos y limitar el potencial de ataques internos.

Desarrollo de un Marco de Seguridad de la Información en el Banco Pichincha

El desarrollo de políticas de seguridad en el Banco Pichincha debe basarse en los fundamentos de COBIT 5, definiendo el alcance de la política, roles y responsabilidades, junto con procedimientos y controles específicos para establecer y mantener la seguridad.

- **Fundamentos**: Según la guía de Pirani Risk (2023), las políticas de seguridad deben garantizar la protección adecuada de todos los activos de información y prevenir riesgos que afecten su confidencialidad, integridad y disponibilidad. Estas políticas deben estar alineadas con los objetivos estratégicos del Banco Pichincha.

- **Alcance de la Política**: La política de seguridad del Banco Pichincha debería ser aplicable a todos los activos de información de la compañía, así como a todos los procesos y actividades de negocio, incluyendo a todas las personas que directa o indirectamente prestan algún servicio para la organización (Pirani Risk, 2023).
- **Roles y Responsabilidades**: Definir roles claros para la gestión de riesgos, incluyendo responsabilidades en seguridad de la información, ciberseguridad y seguridad TI. Esto garantiza el cumplimiento adecuado de la política y del Sistema de Gestión de Seguridad de la Información (Pirani Risk, 2023).

Procedimientos y Controles

- **Establecimiento de Controles**: La implementación de la norma ISO/IEC 27001 permite a las organizaciones identificar los riesgos de seguridad y establecer controles para gestionarlos o eliminarlos. Estos controles deberían ser adaptados para proteger los datos confidenciales del Banco Pichincha y ayudar a lograr un mejor nivel de proveedores preferentes (BSI Group, 2023).
- **Controles Específicos**: La adopción de controles como la autenticación de dos factores, el cifrado de datos y firewalls fortalecerá la seguridad para la empresa y sus clientes, aumentando la conciencia de seguridad y mejorando la documentación e informes.

Gestión de Riesgos de Seguridad

La identificación y gestión de riesgos relacionados con ataques cibernéticos, filtraciones de datos, y fraudes internos son esenciales. El Banco Pichincha debe implementar un plan de mitigación de riesgos que incluya tecnologías de seguridad avanzadas, protocolos de respuesta a incidentes, y auditorías y revisiones continuas.

Identificación de Riesgos:

- **Ataques Cibernéticos**: Los bancos, incluido el Banco Pichincha, son objetivos atractivos para los ciberdelincuentes. Los ataques pueden incluir malware, phishing, y ransomware. Un enfoque proactivo es evaluar continuamente las amenazas emergentes y actualizar las estrategias de defensa.
- **Filtraciones de Datos**: Considerando incidentes pasados en el sector bancario, el Banco Pichincha debe estar atento a posibles filtraciones de datos. Esto implica

monitorear el acceso a la información y detectar cualquier actividad sospechosa que pueda indicar una filtración.

- **Fraudes Internos**: El fraude interno es otro riesgo significativo. Implementar controles de acceso y monitorear las actividades internas puede ayudar a prevenir estos incidentes.

Plan de Mitigación de Riesgos:

- **Adopción de Tecnologías de Seguridad Avanzadas**: Para combatir los ataques cibernéticos, el Banco Pichincha podría implementar sistemas de detección y prevención de intrusiones, firewalls avanzados, y soluciones de seguridad de endpoint. La encriptación de datos y la autenticación multifactor son esenciales para proteger las transacciones y la información del cliente.
- **Protocolos de Respuesta a Incidentes**: Desarrollar un plan de respuesta integral es crucial. Esto incluye procedimientos para la detección rápida, contención, erradicación y recuperación de incidentes. Además, es importante tener un plan de comunicación para informar a los afectados y a las autoridades pertinentes en caso de un incidente.
- **Capacitación y Concienciación**: Realizar programas de formación para los empleados sobre las mejores prácticas de seguridad y cómo reconocer y reportar posibles amenazas. Fomentar una cultura de seguridad es fundamental para prevenir incidentes.
- **Auditorías y Revisiones Continuas**: Llevar a cabo auditorías regulares de seguridad y revisar los controles de seguridad para asegurar su efectividad y hacer ajustes cuando sea necesario.

El análisis realizado por WeLiveSecurity destaca vulnerabilidades críticas en el Banco Pichincha, especialmente en lo que respecta a los riesgos de malware y phishing. Esta revelación subraya la importancia de una vigilancia y prevención eficaces contra estas formas de amenazas cibernéticas en el sector bancario. Los antecedentes del Banco Pichincha en cuanto a incidentes cibernéticos ofrecen insights valiosos sobre los métodos y estrategias utilizados por los atacantes, lo cual es esencial para identificar y reforzar las áreas más susceptibles a ataques.

Aplicación del Plan de Mitigación de Riesgos:

La aplicación efectiva del plan requiere una gestión proactiva de incidentes, mejoras tecnológicas continuas, y auditorías enfocadas en experiencias previas para adaptar y mejorar constantemente las estrategias de seguridad del Banco Pichincha.

- **Gestión Proactiva de Incidentes Anteriores:** Inspirándose en los eventos reportados por WeLiveSecurity, el Banco Pichincha podría enfocarse en establecer un plan comprensivo de respuesta a incidentes. Este plan debe ir más allá de las soluciones técnicas, abarcando también estrategias de comunicación efectiva con los clientes y entidades reguladoras para asegurar la confianza y el cumplimiento normativo.
- **Mejoras Tecnológicas y Educación Continua:** Tomando como referencia los incidentes pasados, una actualización constante de las tecnologías de seguridad es crucial para salvaguardar al banco contra futuros ataques. Además, la formación continua del personal sobre las tácticas en evolución de los ciberdelincuentes es vital para fortalecer la primera línea de defensa del banco.
- **Auditorías Enfocadas en Experiencias Previas:** Las revisiones y auditorías de seguridad deben concentrarse en las áreas previamente comprometidas. Esto asegura que se identifiquen y se corrijan las debilidades, fortaleciendo la seguridad general del banco contra tipos de ataques ya experimentados.

Capacitación y concienciación en seguridad de la información

Un programa de capacitación diseñado para evaluar las necesidades de competencia del personal y abordar áreas críticas de seguridad a través de metodologías diversificadas y evaluación continua asegurará el mantenimiento de la concienciación sobre la seguridad en el Banco Pichincha.

Es importante establecer un programa de capacitación y concienciación en seguridad de la información es vital para reforzar las defensas del Banco Pichincha contra amenazas cibernéticas.

Evaluación de Necesidades y Análisis de Público Objetivo:

- **Diagnóstico de Competencias:** Realizar una evaluación detallada del nivel de conocimiento actual del personal en seguridad de la información, incluyendo una variedad de departamentos y roles.

- **Identificación de Áreas Críticas:** Determinar áreas específicas donde la capacitación es más necesaria, basándose en riesgos y vulnerabilidades identificados previamente.

Diseño del Programa de Capacitación:

- **Contenidos Específicos**: Desarrollar módulos que aborden temas como la seguridad en transacciones en línea, protección contra ingeniería social, políticas de uso aceptable de los recursos de TI, y protocolos de seguridad para trabajo remoto.
- **Metodologías Diversificadas:** Combinar métodos tradicionales de enseñanza con simulaciones interactivas y juegos de roles para mejorar la retención del conocimiento y la aplicación práctica.

Implementación y Participación Activa:

- Planificación de Sesiones: Establecer un calendario de capacitaciones, asegurando la participación de todos los empleados en diferentes horarios y formatos (presencial y online).
- Inclusión de Expertos: Incluir charlas y talleres impartidos por expertos en ciberseguridad para proporcionar insights y consejos prácticos.

Evaluación Continua y Mejora:

- Pruebas de Conocimiento: Implementar pruebas y evaluaciones periódicas para medir la comprensión y aplicación de los conceptos aprendidos.
- Simulacros de Seguridad: Organizar simulacros de ataques cibernéticos y situaciones de riesgo para evaluar la respuesta del personal en escenarios reales.

Mantenimiento de la Concienciación:

- Comunicación Regular: Mantener la seguridad de la información en la mente de los empleados a través de boletines, alertas de seguridad regulares y actualizaciones sobre nuevas amenazas.
- Embajadores de Seguridad: Crear una red de embajadores de seguridad en diferentes departamentos que promuevan las mejores prácticas y actúen como puntos de contacto para dudas y reportes.

El programa de capacitación debe ser un programa integral y continuo de capacitación y concienciación en seguridad de la información es clave para fortalecer la postura de seguridad del Banco Pichincha. A través de este programa, los empleados estarán mejor equipados para reconocer y responder a amenazas cibernéticas, contribuyendo así a la protección de los activos y la reputación del banco.

Propuesta de Mecanismos de Control de Riesgos y Evaluación Continua Alineados con COBIT para el Sector Financiero Bancario en Ecuador

1. **Establecimiento de Mecanismos de Control de Riesgos:**
    - **Adopción de un Marco Integral de Gobernanza de Riesgos:** Implementar un marco de gobernanza de riesgos basado en COBIT que abarque la identificación, evaluación, mitigación y monitoreo de riesgos. Esto incluye riesgos tecnológicos, operativos y de cumplimiento.
    - **Controles de Seguridad de la Información:** Aplicar controles de seguridad alineados con APO13 de COBIT, como la autenticación multifactor, encriptación de datos y firewalls**.**
2. **Desarrollo de Procedimientos para la Evaluación Continua:**
    - **Auditorías y Revisiones Regulares:** Establecer un cronograma de auditorías internas y externas para revisar la efectividad de los controles y políticas de seguridad.
    - **Evaluaciones de Conformidad:** Realizar evaluaciones periódicas para asegurar la conformidad con normativas locales e internacionales relevantes para el sector bancario.
3. **Implementación de Indicadores o KPIs Alineados con COBIT:**
    - **KPIs de Seguridad de la Información:** Establecer KPIs como el número de incidentes de seguridad resueltos, tiempo promedio para detectar y responder a incidentes y el porcentaje de cumplimiento de las políticas de seguridad.
    - **KPIs de Gobernanza y Cumplimiento:** Medir la efectividad de la gobernanza de TI con KPIs como el nivel de cumplimiento normativo y la satisfacción del usuario final con los servicios de TI.
4. **Alineación con los Requisitos del Sector Financiero en Ecuador:**

- **Adaptación a la Regulación Local:** Asegurarse de que todos los mecanismos de control y KPIs estén en conformidad con las regulaciones de la Superintendencia de Bancos de Ecuador.
- **Enfoque en la Protección de Datos del Cliente:** Dado el manejo de datos financieros sensibles, los controles deben enfocarse especialmente en la privacidad y seguridad de los datos del cliente.

KPIs alineados específicamente para Banco Pichincha y adaptados a las directrices de la Superintendencia de Bancos en Ecuador:

Los siguientes KPIs están diseñados para proporcionar una visión clara del rendimiento y la conformidad de las operaciones del Banco Pichincha en áreas clave de seguridad, gestión de riesgos, operaciones de TI y continuidad del negocio, teniendo en cuenta tanto las mejores prácticas de COBIT como las regulaciones específicas del sector bancario en Ecuador.

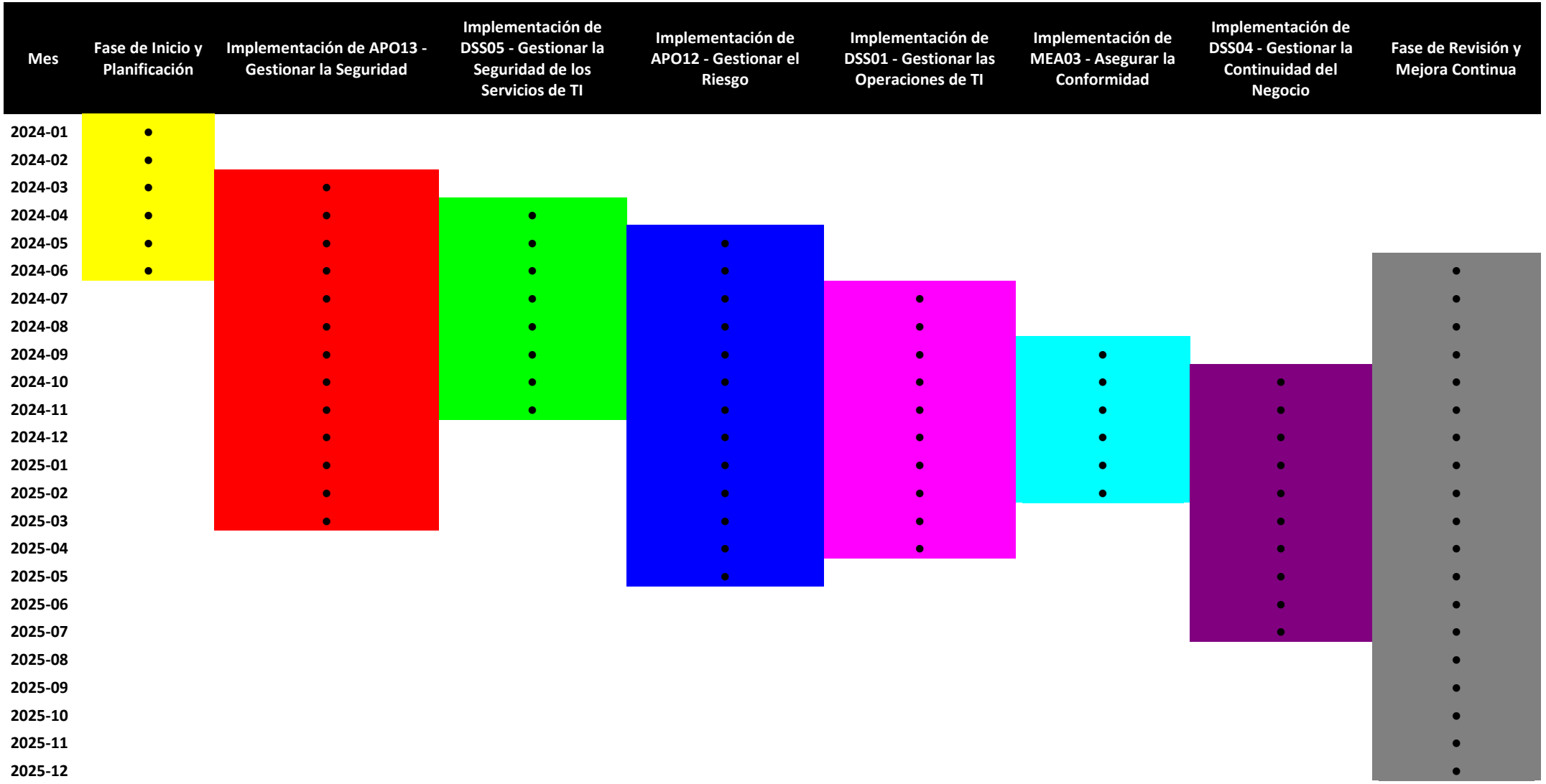
Tabla 5

KPIs alineados específicamente para Banco Pichincha y adaptados a las directrices de la Superintendencia de Bancos en Ecuador (Elaboración propia, 2024).

KPI son las siglas de "Key Performance Indicator"	
APO13 - Gestionar la Seguridad	• **Número de Incidentes de Seguridad Relacionados con Transacciones Financieras:** Cantidad de incidentes de seguridad informáticos detectados que afectan directamente las transacciones financieras en un período específico. • **Porcentaje de Resolución de Incidentes de Seguridad en Tiempo:** Proporción de incidentes de seguridad gestionados dentro del tiempo objetivo establecido por políticas internas y regulaciones de la SB.
DSS05 - Gestionar la Seguridad de los Servicios de TI	• **Tiempo de Inactividad de Sistemas Críticos Bancarios por Problemas de Seguridad:** Medición del tiempo total de inactividad de los sistemas críticos de banca debido a fallas de seguridad. • **Número de Violaciones de Seguridad en Aplicaciones de Banca Móvil o en Línea:** Cantidad de violaciones de seguridad específicas en aplicaciones de banca móvil o en línea.
	• **Número de Riesgos Financieros Identificados y Gestionados:** Comparación entre los riesgos financieros identificados y los que han sido mitigados, enfocándose en aspectos como el fraude, la liquidez y el crédito.

APO12 - Gestionar el Riesgo	• **Impacto Financiero de Riesgos No Mitigados:** Evaluación del impacto financiero en el banco de riesgos que no fueron mitigados efectivamente.
DSS01 - Gestionar las Operaciones de TI	• **Índice de Disponibilidad de Sistemas Bancarios Clave:** Porcentaje de tiempo en que los sistemas bancarios críticos están operativos y disponibles para los clientes y empleados. • **Tiempo Promedio de Resolución de Problemas en Sistemas de TI:** Tiempo promedio que tarda el equipo de TI en resolver problemas en los sistemas bancarios.
MEA03 - Asegurar la Conformidad con Políticas y Normas Externas	• **Número de Hallazgos de Conformidad en Auditorías Externas:** Cantidad de hallazgos o áreas de mejora identificados en auditorías externas relacionadas con las regulaciones de la Superintendencia. • **Porcentaje de Cumplimiento con Normativas de Protección de Datos del Cliente:** Proporción de controles y políticas que cumplen con las regulaciones de protección de datos del cliente.
DSS04 - Gestionar la Continuidad del Negocio	• **Efectividad de los Ejercicios de Continuidad del Negocio:** Resultados y lecciones aprendidas de las pruebas periódicas del plan de continuidad del negocio. • **Tiempo de Recuperación Objetivo (RTO) para Servicios Críticos:** Medición de cuán efectivamente el banco puede recuperar servicios críticos tras un incidente, en línea con los objetivos establecidos.

Cronograma de Implementación de Procesos de COBIT en el Banco Pichincha (Roadmap)



Conclusiones

- La adopción del marco COBIT por parte de las instituciones financieras en Ecuatoriano es fundamental para alienar las actividades de tecnologías de la información (TI) con las directrices estratégicas de estas instituciones. Este proceso permite que el uso de tecnologías no solo se limite a cumplir con las exigencias operativas diarias, sino que también contribuya de manera significativa al logro de los objetivos comerciales establecidos. Implementar COBIT permite a los optimizar su gobernanza y administración de TI, un aspecto crítico en el contexto actual, donde la digitalización y las normativas específicas del sector financiero están en constante evolución.
- COBIT facilita una mayor alineación entre las operaciones de TI y los objetivos estratégicos de una organización. En el ejemplo desarrollado, al enfocarse en prácticas que son críticas para el Banco Pichincha, se garantiza que la tecnología de la información actúe como un habilitador clave para alcanzar metas empresariales, mejorar la eficiencia operativa y fomentar la innovación.
- La implementación de prácticas de COBIT seleccionadas según las regulaciones específicas del sector bancario en Ecuador y normativas internacionales relevantes fortalece el cumplimiento normativo. Esto no solo reduce el riesgo de sanciones y multas, sino que también aumenta la confianza de los clientes y partes interesadas en la seguridad y estabilidad del banco.
- Personalizar COBIT ayuda a integrar la seguridad de la información y las mejores prácticas de TI en la cultura organizacional, además promueve una mayor conciencia y comprensión de la importancia de la seguridad y la gobernanza de TI entre todos los empleados, reforzando las defensas del banco contra riesgos internos y externos.

Recomendaciones:

- Es crucial que se realicen evaluaciones continuas de su implementación de COBIT para asegurar su relevancia y efectividad a lo largo del tiempo. Adaptarse a las cambiantes tecnologías y regulaciones es fundamental para mantener una gobernanza de TI robusta.
- Asegurar el compromiso y apoyo de la alta dirección es esencial para el éxito de la implementación personalizada de COBIT. La gobernanza de TI debe ser vista como una prioridad estratégica a nivel ejecutivo.

- Invertir en programas de capacitación y concienciación sobre las prácticas de COBIT, seguridad de la información y gobernanza de TI fortalecerá las capacidades internas del banco y promoverá una cultura de seguridad.

REFERENCIAS

[1]. Eito-Brun, R. & Calleja Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: Presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. Revista Española de Documentación Científica, 43 (3), e272. Recuperado de https://doi.org/10.3989/redc.2020.3.1666

[2]. García. H. (1016). Propuesta de un modelo de arquitectura de organización para la gestión de TIC´S en las PYMES (Publicación No. CD-6885). Escuela Politécnica Nacional, Quito, Ecuador, Recuperado de https://bibdigital.epn.edu.ec/

[3]. Lanter, D. COBIT 2019 Framework: Introduction and Methodology (2019). ISACA, Rolling Meadows, IL: ISACA Recuperado de https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

[4]. Smallwood, R. F. (2019). Information Governance, IT Governance, Data Governance: What's the Difference? , Information Governance (pp. 19-28). DOI:10.1002/9781119491422.ch2

[5]. Strait, C. (2010). Building a business case for records management. ISACA Journal, vol. 6, 1-3. Recuperado de https://redc.revistas.csic.es/index.php/redc/article/view/1297

[6]. Carmona Ramírez, C. M. (2013). Modelo de gobernabilidad basado en COBIT para la gestión por procesos definida en un espacio multidimensional. Universidad de Medellín. Recuperado de https://repository.udem.edu.co/handle/11407/43

[7]. Oblitas, A., & Sota, L (2019, 13 de junio). Aplicación de COBIT 5 en la gestión y gobernabilidad de las tecnologías de información y comunicación, para generar valor agregado y competitividad en la atención al cliente del proceso crediticio de la Caja Municipal Arequipa – Filial Cusco (Publicación No. CD-3932), Tesis de pregrado, Universidad Andina del Cusco. Recuperado de https://repositorio.uandina.edu.pe/handle/20.500.12557/3932

[8]. Eito-Brun, R., & Calleja Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. Revista española de documentación científica, 43(3). Recuperado de https://redc.revistas.csic.es/index.php/redc/article/download/1297/2018?online

[9]. Ferro, R., & Tarazona, G. (2015). Implementación de procedimientos de gobernabilidad TI en la red de investigación de tecnología avanzada

basado en ITIL, COBIT y la ISO 20000-27000. Vol. 6 (2015). DOI: https://doi.org/10.14483/2248762X.8501

[10]. De la Cruz, P.(2017). Capital intelectual, gestión del conocimiento en la interacción gobierno y gestión de las tecnologías de la información desde la perspectiva COBIT 5. Vol. 4, Núm. 2 (2017). Semestral de divulgación científica española de documentación científica, Recuperado de https://dialnet.unirioja.es/descarga/articulo/6230648.pdf

[11]. Orellana, X., & Álvarez, M (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. Polo del Conocimiento. Recuperado de https://orcid.org/0000-0003-3699-3406

[12]. Velásquez, T., Puentes, A., & Pérez., Y.(2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. Tecnura, 19, 159-169. doi: 10.14483/udistrital.jour.tecnura.2015.SE1.a14

[13]. Banco Mundial. (2021, 12 de noviembre). Sector financiero. Banco Mundial BIRF AIF. https://www.bancomundial.org/es/topic/financialsector/overview#:~:text=Los%20sistemas%20bancarios%20y%20mercados,a%20trav%C3%A9s%20de%20las%20fronteras.

[14]. Mis Finanzas para Invertir. (2023, 1 de febrero). ¿Por qué son importantes los bancos para la sociedad? https://www.misfinanzasparainvertir.com/por-que-son-importantes-los-bancos-para-la-sociedad/

[15]. Danby, S. (2023, 17 de abril). Gobernanza IT: definición, marcos y mejores prácticas. IT Management Software. https://blog.invgate.com/es/gobernanza-it#:~:text=Su%20objetivo%20es%20ayudar%20a,necesidades%20de%20las%20partes%20interesadas.

[16]. Cordova, A. (2014). Identificación de los factores y eventos de riesgo operativo dentro del proceso de gestión de tecnologías de información y comunicación basado en COBIT 5.0 en instituciones públicas, caso Banco del Estado (Tesis de maestría). Escuela Politécnica Nacional. Repositorio EPN.

[17]. Arias, J. (2011). Hacia la planeación estratégica en Tecnologías. Bucaramanga: Fundación Universitaria Católica del Norte

[18]. Unacademy. (2023, 28 de agosto). Kerala PSC Science & Technology Study Material: ICT. Recuperado de https://unacademy.com/content/kerala-psc/study-material/science-technology/ict/

[19]. Rodrigues, N. (2023, 20 de enero). PMBOK: qué es, para qué sirve, fases y herramientas. HubSpot. https://blog.hubspot.es/sales/que-

es-pmbok

[20]. Netmind. (2023, febrero). Lean IT a la Práctica (Incluye Lean IT Foundation). Netmind. https://netmind.net/es/curso/lean-it-a-la-practica-incluye-lean-it-foundation/#:~:text=Lean%20IT%20es%20la%20extensi%C3%B3n,se%20dirige%20a%20proporcionar%20valor.

[21]. Velastegui Sanchez, T. A. (2007). Análisis de la gestión de la tecnología de la información en la unidad de gestión de la información de la Escuela Politécnica Nacional utilizando COBIT. (Tesis de grado). Escuela Politécnica Nacional. Repositorio EPN.

[22]. Cordero Calderón, M. I., & Ibujés Rivera, M. C. (2008). Auditoría de Riesgos informáticos del departamento de sistemas de Teleamazonas usando COBIT. (Tesis de grado). Escuela Politécnica Nacional. Repositorio EPN.

[23]. Arias, J. (2011). Hacia la planeación estratégica en Tecnologías . Bucaramanga: Fundación Universitaria Católica del Norte.

[24]. Espinoza, C. B. (2018). Gobierno de Tecnologías de la Información (TI) como aliado del Negocio: Marco de Gobierno de Tecnologías de la Información . España: Editorial Académica Española.

[25]. IT Governance Institute. (2008). IT Governance Global Status Report—2008. USA: IT Governance Institute.

[26]. Rodríguez, D. (2018). Gestión de disponibilidad de los servicios . Lima: Universidad Peruana de Ciencias Aplicadas (UPC).

[27]. Velásquez, M., Castillo, P. G., & Zambrano, M. E. (2016). Planificación estratégica de tecnologías de la información y comunicación. Dom. Cien, 560-570

[28]. Cabero, J. (1996). Nuevas tecnologías, comunicación y educación. EDUTEC. Revista Electrónica de Tecnología Educativa, 1. Recuperado de http://www.uib.es/depart/gte/revelec1.htm

[29]. Superintendencia de Bancos. (2023). Recuperado de C

[30]. Asobanca. (2022). El sistema bancario apuesta por la inclusión financiera en Ecuador. Recuperado de https://asobanca.org.ec/sistema-bancario-inclusion-financiera-ecuador/

[31]. Superintendencia de Bancos. (2021). Resolución No. SB-2021-2003. Coordinación General de Tecnologías de Información y Comunicación, Dirección de Gobernanza de TI e Innovación. Plan estratégico de tecnologías de información y comunicación (PETIC).

[32]. G. Saba, «El Arte de la Seguridad de la Información en la Globalización», Revista PGI. Investigación, Ciencia y Tecnología en Informática, nº 8, pp. 77-79, 2020.

[33]. PowerDMARC. (2023). Ciberseguridad en el sector bancario: Principales amenazas y prevención. Recuperado de https://www.powerdmarc.com/ciberseguridad-en-el-sector-bancario-principales-amenazas-y-prevencion/

[34]. IT ahora. (2019). MDM visión 360 es parte de la transformación digital de Banco Pichincha. Recuperado de https://www.itahora.com/mdm-vision-360-es-parte-de-la-transformacion-digital-de-banco-pichincha/

[35]. Banco Pichincha. (2023). Seguridad en Internet. Recuperado de https://www.pichincha.com/seguridad/internet

[36]. Pirani Risk. (2023). *Guía para hacer una Política de Seguridad de la Información*. Recuperado de https://www.piranirisk.com/guia-para-hacer-una-politica-de-seguridad-de-la-informacion

[37]. BSI Group. (2023). *Casos prácticos de ISO/IEC 27001: Seguridad de la Información*. Recuperado de https://www.bsigroup.com

[38]. Radio Pichincha. (2021). Fallas en sistema electrónico afectan nuevamente a usuarios de Banco Pichincha. Recuperado de https://www.radiopichincha.com