UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERIAS

"METODOLOGÍA DE AUDITORÍA INFORMÁTICA PARA EVALUAR EL ÁREA DE CONTROL DE CALIDAD DE SOFTWARE EN BANCOS PRIVADOS MEDIANOS DEL ECUADOR, BASADA EN EL MARCO DE REFERENCIA COBIT"

Realizado por:

Henry Humberto Vargas García

Director del proyecto:
Ing. Mónica Romero, Mgt

Como requisito para la obtención del título de:
MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

DECLARACIÓN JURAMENTADA

Yo, HENRY HUMBERTO VARGAS GARCIA, con cédula de identidad número 020163560-4, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Henry Humberto Vargas García
C.C: 020163560-4

DECLARATORIA

El presente trabajo de investigación titulado:

“METODOLOGÍA DE AUDITORÍA INFORMÁTICA PARA EVALUAR EL AREA DE CONTROL DE CALIDAD DE SOFTWARE EN BANCOS PRIVADOS MEDIANOS DEL ECUADOR, BASADA EN EL MARCO DE REFERENCIA COBIT”

Realizado por:

HENRY HUMBERTO VARGAS GARCÍA

Como requisito para la Obtención del Título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

ha sido dirigido por la profesora

Ing. MONICA ROMERO PAZMIÑO, Mgt

quien considera que constituye un trabajo original de su autor

Mónica Romero Pazmiño

DIRECTOR

PROFESORES INFORMANTES

Después de revisar el trabajo presentado, lo ha calificado como apto para su defensa oral ante el tribunal examinador

_____ _____

ING. Diego Riofrío Luzcando **ING. Fabian Hurtado**

DEDICATORIA

Dedico este trabajo a mi esposa Alexandra y mi hija Melissa, quienes han estado siempre a mi lado brindándome el ánimo y el apoyo en momentos difíciles y que además han sabido entender y compartir el sacrificio que implica conseguir nuevas metas.

A mis padres Humberto y Gloria, que con su ejemplo e interminable apoyo han contribuido para poder cumplir con cada una de las metas que me he propuesto para llegar a ser un profesional de bien.

Una mención especial para mis suegros Hernán y Teresa, quienes han dedicado su tiempo y esfuerzo a entregarme los mejores consejos de vida que me han guiado al momento de enfrentar retos como los que me he propuesto, hasta llegar a una feliz consecución.

AGRADECIMIENTOS

Quiero agradecer en primer lugar a Dios por ser mi fortaleza espiritual en todos los actos de mi vida, y luego a todos los profesores de la Maestría en Tecnologías de la Información de la Universidad Internacional SEK, de quienes recibí sus conocimientos y experiencias, principalmente a la Magister Mónica Romero por su paciencia y respaldo en varios pasajes de la carrera y principalmente como Directora de Tesis supo guiarme y motivarme a cumplir de la mejor manera con la presentación de este trabajo.

Agradezco a mi familia y amigos, que compartieron momentos de intranquilidad y preocupación y de quienes recibí el aliento para seguir adelante hasta culminar con éxito el reto planteado, mi más sincero a agradecimiento a todos.

RESUMEN

En el Ecuador, las entidades financieras están más enfocadas en mejorar sus canales de atención, entre ellos el digital, ya que permite mejorar los procesos internos y externos de los bancos. Con base en estas necesidades, la presente investigación tiene como objetivo principal crear una metodología de auditoría informática dirigida a evaluar el área de Control de Calidad de Software en bancos privados medianos del Ecuador.

Para obtener información, que sirve de sustento para el desarrollo de esta propuesta, se ha tomado como referencia un banco mediano de Ecuador, donde ha habido fallas en las etapas de ciclo de certificación de un sistema, dando como resultado un software de baja calidad. Para proveer una solución a esta problemática, se propone diseñar una herramienta destinada a evaluar el área de Calidad de Software mediante la identificación de procesos, métodos, actividades y controles que se ejecutan en el área, para luego, con base en el Marco de referencia COBIT relacionarlos con los dominios de COBIT.

Finalmente, el diseño de la metodología propuesta se completa con la descripción de las fases a seguir y cumplir al momento de ejecutar la auditoría. Cada fase se presenta de manera práctica y sencilla de tal manera que puedan ser entendida, ya sea por auditores expertos como por aquellos que están iniciando en los procesos de ejecución de auditorías.

Palabras clave: Metodología, Calidad, COBIT, Auditoría, Sistema, Estándares de calidad, Normas de calidad, Entidad financiera.

ABSTRACT

In Ecuador, financial entities are more focused on improving their attention channels, among them the digital, since it allows improving the internal and external processes of banks. Based on these needs, the present investigation has as main objective to create a methodology of computer audit aimed at evaluating the area of Software Quality Control in medium-sized private banks in Ecuador.

To obtain information, that serves as sustenance for the development of this proposal, a medium bank of Ecuador has been taken as a reference, where there have been failures in the stages of the certification cycle of a system, giving as result low quality software. To provide a solution to this problematic, it is proposed to design a tool to evaluate the area of Software Quality by identifying processes, methods, activities and controls that are executed in the area, and then, based on the COBIT Reference Framework, relate them to the COBIT domains.

Finally, the design of the proposed methodology is completed with the description of the phases to follow and comply when executing the audit. Each phase is presented in a practical and simple way in such a way that they can be understood for its application, either by expert auditors or by those who are starting in the audit execution processes.

Keywords: Methodology, Quality, COBIT, Audit, Software, Quality standards, Quality rules, financial entities.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS Y FIGURAS

INDICE DE FIGURAS

CAPÍTULO I

INTRODUCCIÓN

1.1. PROBLEMA DE LA INVESTIGACIÓN

1.1.1. Planteamiento del problema

Las empresas en general y más aún las entidades financieras en el Ecuador, buscan dar mayor facilidad de acceso al cliente a sus productos y servicios a través de diversos medios como son los canales digitales. El cliente tiene la posibilidad de realizar sus transacciones de manera rápida y efectiva mientras que la entidad ofrece más y mejores servicios que generen rentabilidad.

Existen diversos estándares de calidad del software como: ISO 9000, ISO 9001, ISO 9002, ISO 9003, ISO 9004, ISO 9126, ISO 20000, IEEE 730-2003, IEEE 829-1998, etc. Que han sido propuestos por entidades como la Organización Internacional de Normalización (ISO) que se compone de distintas organizaciones de estandarización a nivel mundial y el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) quienes han generado estándares aplicables a productos de software (Scalone, 2006). Si bien estos estándares ilustran de manera amplia, técnica y ordenada sobre los elementos a tener en cuenta para una adecuada gestión de la tecnología de información, estos no orientan de manera específica sobre los procedimientos a seguir para una auditoría integral a la gestión de calidad de los cambios tecnológicos implementados. Esto origina que no exista una adecuada evaluación de los procesos que se siguen para garantizar que los nuevos desarrollos tecnológicos en entidades financieras sean de calidad y no se produzcan errores una vez que se implementan en producción.

1.1.2. Diagnóstico del Problema

Las entidades financieras del Ecuador como son los bancos, donde un gran número de clientes están interactuando en agencias, oficinas, centros de atención telefónica o a su vez por medios electrónicos, necesitan mantener toda su infraestructura y sus aplicativos funcionando las 24 horas durante los 365 días del año. Esto se puede

convertir en un gran problema si los sistemas internos o los que están expuestos vía online, presentan fallas debido a que fueron implementados sin haber cumplido un proceso de pruebas de calidad del software que garantice su correcto funcionamiento.

Es importante que exista una forma de identificar los problemas que se presentan al momento de ejecutar pruebas para determinar la calidad del Software desarrollado. Una forma de hacerlo es mediante una auditoría informática que sea guiada por una metodología práctica para un área específica, que incluya la verificación de cada una de las actividades que intervienen para generar una certificación sobre el desarrollo de cualquier aplicación desde su inicio hasta su fin. La metodología ayudará a determinar dónde y que proceso está fallando, para aplicar los correctivos necesarios a fin de garantizar la calidad de los sistemas que son expuestos a los usuarios internos de una entidad y al público en general, previo a su puesta en funcionamiento en un ambiente productivo.

Para conocer la problemática presente fue de gran ayuda pedir información al personal que forma parte del área de control de calidad de software de un banco clasificado como mediano en el país (Superintedencia de Bancos Portal Estadístico, 2018). Alejandro Javier Ushca Flores, quien trabaja en el área como Analista de Pruebas QA, colaboró para la obtención de información sobre cuatro aspectos (Ambiente de pruebas, Personas, Proceso de pruebas y Capacidad del servicio) analizados para reconocer posibles causas que generan fallas en las diferentes etapas de ciclo de certificación de un sistema. Su experiencia y conocimiento permitieron entender de mejor manera esta problemática e incluso crear un diagrama causa efecto con los hallazgos obtenidos.

Según la Superintendencia de Bancos del Ecuador, en su Boletín Mensual de Julio del 2018, revela las cifras de los bancos considerados grandes, medianos y pequeños. De las 23 entidades financieras que controla la Superintendencia de Bancos en Ecuador, nueve son los bancos privados considerados medianos, siendo uno de los aspectos que evalúa el monto en activos con el que cuenta cada entidad financiera (Superintedencia de Bancos Portal Estadístico, 2018).

CUENTA	BP AUSTRO	BP BOLIVARIANO	BP CITIBANK	BP DINERS	BP RUMIÑAHUI	BP INTERNACIONAL	BP LOJA	BP MACHALA	BP SOLIDARIO
ACTIVO	1684958,8	3172588,25	652931,18	1909688,6	807351,66	3426261,95	454001	744470,91	754455,46
% de participación del activo en el sistema	4,34	7,99	1,65	4,3	2,13	9,13	1,15	1,79	1,85

Tabla .- Reporte mes de Julio 2018 Superintendencia de Bancos del Ecuador

Fuente:(Superintendencia de Bancos Portal Estadístico, 2018)

Diagrama Causa-efecto

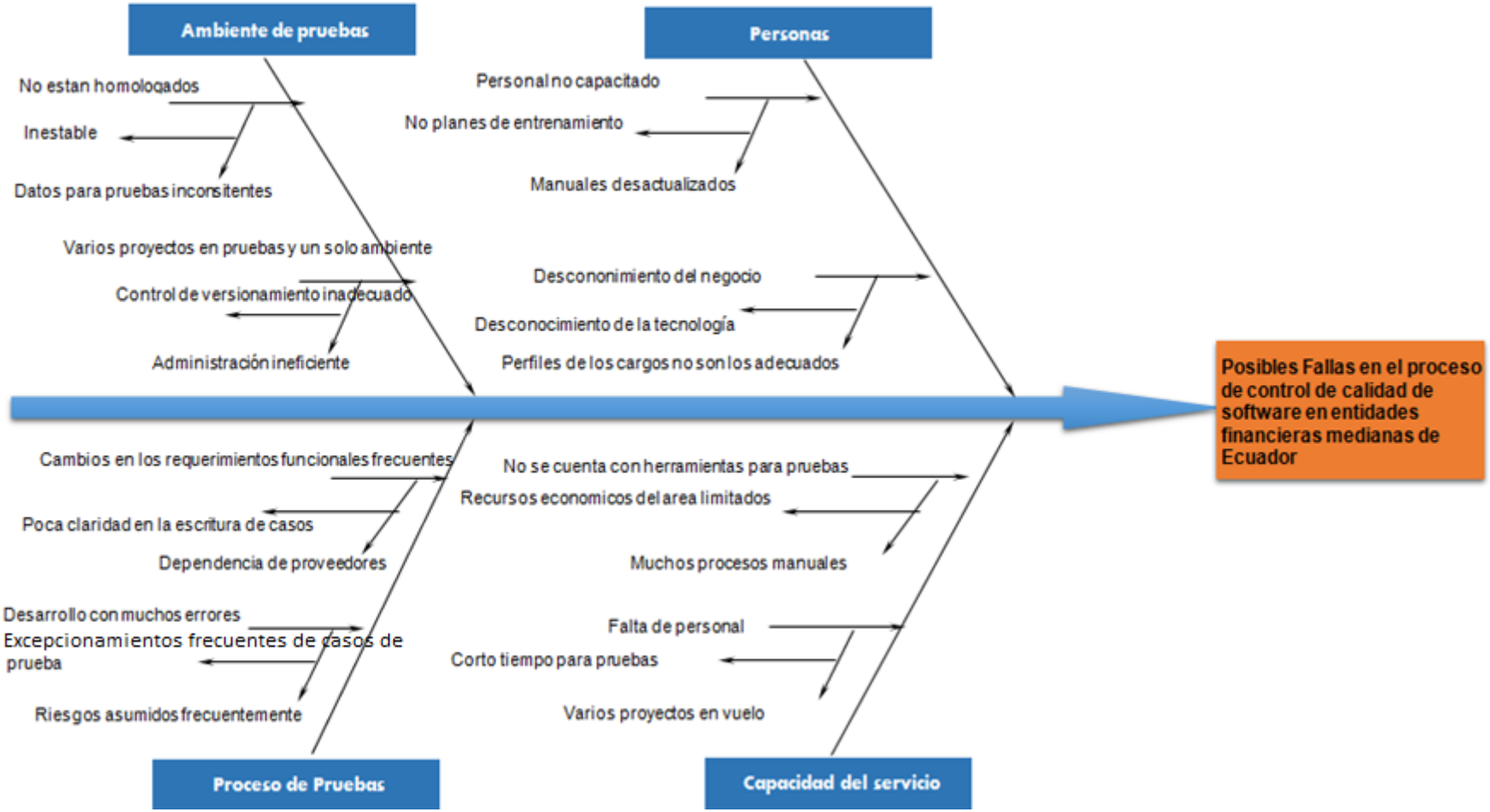


Figura . Posibles causas que ocasionan problemas en el Área de Calidad de Software.

Fuente: Autor de la Investigación.

El diagrama refleja las causas que generan problemas en los procesos del área de Calidad de Software, mostrando la necesidad de una evaluación a través de una auditoria informática, que utilice una metodología que considere practicas dirigidas a conocer el estado de los procesos del área, de modo que se pueda encontrar las fallas presentes que provocan inconformidades de los sistemas una vez puestos en producción y que además entregue a los interesados las recomendaciones para que se generen soluciones.

Es probable que la falla de un sistema informático no pueda ser corregida, porque no se ha ejecutado una auditoria o porque al ejecutarla, no se enfocó directamente en los procesos que son parte del área. Para lograr la orientación requerida, se plantea una metodología de auditoria dirigida a evaluar expresamente lo relacionado con la calidad de software, por esta razón se hace necesario conocer cuáles son los procesos y priorizarlos determinando su criticidad.

El esquema metodológico de auditoría planteado está basado en las buenas prácticas que propone el Marco de Referencia COBIT para la ejecución de auditorías informáticas.

1.1.3. Formulación del Problema

La falta de una metodología de auditoría informática para evaluar expresamente el área de calidad de software en bancos privados medianos en Ecuador, puede ser un factor que influya para que los procesos que se siguen en el área, durante la ejecución del ciclo de pruebas de un sistema sean deficientes.

1.2. OBJETIVOS

1.2.1. Objetivo General

Diseñar una metodología de auditoría informática para la evaluación del área de control de calidad de software en bancos medianos del Ecuador, basada en el Marco de referencia COBIT.

1.2.2. Objetivos Específicos

- Recopilar información que contenga una breve descripción de los procesos que son parte del área de Calidad de Software y la problemática presente.
- Analizar los dominios y objetivos de control de COBIT, que apliquen para la evaluación de los procesos del área de calidad de software de bancos privados medianos del Ecuador.
- Proponer una metodología de auditoría informática al área de control de calidad de software de bancos privados medianos en Ecuador, con la ayuda del Marco de Referencia COBIT.
- Socializar la metodología propuesta a personas que trabajan en el área de calidad de software de un banco mediano del Ecuador.
- Evaluar a través de una encuesta aplicada a las personas que reciben la información, el grado de aceptación de la metodología propuesta.

1.3. JUSTIFICACIÓN

Las empresas en general para mantener operativos sus sistemas de forma permanente exigen que sus procesos y desarrollos tecnológicos sean de calidad. Para lograr este objetivo, se debe realizar pruebas para certificar productos de software que cubran los requerimientos y necesidades del negocio; cumpliendo con un control de calidad que mantenga procesos eficientes y puedan ser evaluados mediante una auditoria informática, ejecutada con la ayuda de una metodología adecuada que determine con base en los resultados, que procesos necesitan ser mejorados.

Esta investigación pretende generar una metodología de auditoría informática, orientada a validar los procesos que intervienen al momento de generar una certificación funcional y que son parte importante para garantizar la calidad de software en bancos medianos en el Ecuador. Se espera también aportar positivamente para futuros trabajos sobre temas similares, ya que es un proyecto generado con fines académicos.

Según lo indicado por Piattini y del Peso (2007), la calidad se muestra como una característica importante a cumplir en un mercado cada vez más competitivo, teniendo como

objetivo el beneficio del consumidor final, convirtiéndose en un filtro que las organizaciones experimentan para mantenerse en el mercado.

También se hace referencia al valor que le da a una organización, el tener una función operativa de auditoría informática, que incluya procedimientos de control suficientes para asegurar el funcionamiento de los sistemas informáticos y evaluar dichos controles para determinar si un sistema informático es confiable. La auditoría informática es más valiosa aún en el sector financiero, ya que un error informático puede tener un gran impacto por el número de operaciones que puede llegar a ser afectadas y la repercusión económica que esto implicaría.(Piattini & del Peso, 2007)

El control a la calidad de software juega un papel muy importante dentro de las entidades financieras. Un control de calidad efectivo ayuda a garantizar que se cumplan las metas del negocio, se optimice la inversión y se administre de forma adecuada los riesgos asociados al desarrollo de nuevos sistemas tecnológicos.(Institute IT Governance, 2005)

De acuerdo con las citas mencionadas, se ve factible poder desarrollar un proyecto que logre evidenciar los posibles riesgos del área de control de calidad, así como también la generación de contramedidas para mitigarlos. Mediante la metodología propuesta se dotará de una herramienta que permita a las áreas de control de calidad conocer, asumir y gestionar los procesos de una forma documentada y estructurada, logrando con ello la detección de fallas de forma oportuna. De igual manera, se podrán beneficiar los profesionales de TI, así como las organizaciones que apoyan el desarrollo de nuevas tecnologías, para brindar una mejor atención interna y externamente.

1.4. MARCO TEÓRICO

1.4.1. Auditoría

1.4.1.1. Definición de Auditoría

La definición de auditoría es presentada de varias maneras:

Para Piattini y Del Peso (2007), la auditoría consiste realizar una evaluación en una organización, de la eficacia de los procesos de gestión de riesgos y control, para aportar valor

y mejora en la ejecución de los procesos mediante las recomendaciones que se generen como resultado de la auditoría.

Según Muñoz (2002), es una revisión independiente de una o varias actividades, funciones específicas, resultados de una entidad administrativa, que es ejecutada por una persona capacitada en temas de auditoría, con el fin de evaluar que se realicen de una forma correcta, para luego con base en el análisis realizado, poder emitir opiniones razonables de los resultados.

En cambio, para Huesca (2005) la palabra auditoría se la ha empleado de forma incorrecta, ya que se ha entendido como la evaluación que busca detectar errores y señalar fallas, sin embargo, la auditoría va más allá y busca evaluar la eficiencia de una sección o de un organismo.

1.4.1.2. Definición de Auditoría de Sistemas

Se define como el proceso que se sigue para la recolección y evaluación de la evidencia con el objetivo de determinar si los Sistemas de Información (SI) y los recursos que están relacionados cumplen con la función de proteger los activos, mantener la integridad y disponibilidad de los datos, proporcionando información confiable y útil para la organización. La auditoría de una aplicación hace parte de la Auditoría de Sistemas de Información, refiriéndose a la verificación de cada control que es parte de una aplicación y que son utilizados para garantizar la exactitud de los registros.

Una auditoría de aplicaciones se puede realizar cuando:

- El sistema se evalúa para su adquisición
- Antes de la entrada a producción de un sistema
- Después de haberse puesto en producción el sistema (ISACA, 2011)

1.4.1.3. Fases o etapas de la Auditoría de Sistemas

Según Muñoz (2002), como parte de una metodología de auditoría, que puede ser aplicada para cualquier tipo de auditoría dentro del campo de sistemas se señala tres principales fases o etapas:

- **Planeación de la auditoría:** que comprende identificar el origen de la auditoría, realizar una visita preliminar al área que será evaluada, establecer los objetivos de la auditoría, determinar los puntos que serán evaluados en la auditoría, elaborar planes, programas y presupuestos para realizar la auditoría, identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría y por ultimo asignar los recursos y sistemas computacionales para la auditoría.
- **Ejecución de la auditoría:** en esta etapa se realizan las acciones programadas para la auditoría, aplicando los instrumentos y herramientas que se seleccionaron en la etapa anterior. Además, se identifican y elaboran los documentos de desviaciones encontradas, con el fin de elaborar el dictamen preliminar que integrará el legajo de papeles de trabajo de la auditoría.
- **Dictamen de la auditoría:** las principales acciones a realizar en esta etapa es el análisis de la información para la elaboración de un informe de situaciones detectadas que se registraran en un dictamen final a ser presentado como el informe del auditor (Muñoz, 2002).

1.4.2. Descripción conceptual de metodologías de auditoría informática

El presente trabajo se enfoca en diseñar una metodología de evaluación al área de calidad de software en entidades financieras, por tal motivo y una vez conocido el concepto de auditoría, es importante conocer cómo se lleva a cabo la evaluación en cualquier área mediante una serie de acciones y procedimientos metodológicos específicos, los mismos que deberán ser diseñados previamente de acuerdo con conceptos y lineamientos tal y como se presenta a continuación:

1.4.2.1. Metodología de Auditoría

Que es descrita como un conjunto de procedimientos documentados diseñados para alcanzar objetivos de auditoría planeados. Se compone del alcance, objetivos y programas de auditoría. Debe ser aprobada por la gerencia de auditoría y comunicada al personal que hace parte de la auditoría.

Esta presentada en fases que considera como producto inicial del proceso, un programa de auditoría que va a ser una guía en la ejecución y documentación de los pasos siguientes en el proceso de auditoría (ISACA, 2011).

Las fases que se consideran son las siguientes:

Fase de auditoría	**Descripción**
Sujeto de la auditoría	- Identificar el área que será auditada
Objetivo de la auditoría	- Identificar el propósito de la auditoría. Un ejemplo puede ser verificar que los cambios al código fuente de un sistema se realicen en un ambiente definido
Alcance de la auditoría	- Identificar los sistemas específicos, la función de la organización que se incluye en la revisión. En el ejemplo de cambio a un programa, el alcance se puede limitar a revisar un solo sistema en un periodo de tiempo
Planeación de auditoría	- Identificar las habilidades y recursos técnicos - Identificar las fuentes de información a ser revisadas tales como organigramas funcionales, políticas, estándares, procedimientos y documentación de auditorías previas - Identificar los lugares a ser auditados
Procedimientos de auditoría y pasos para la recopilación de datos	- Seleccionar el método de auditoría para verificar los controles - Buscar las personas para entrevistas - Identificar y obtener las políticas, estándares y directrices de los departamentos para su revisión

	- Desarrollar herramientas y metodologías de auditoría para comprobar y verificar los controles
Procedimientos para evaluar la prueba o revisar los resultados	- La que sea especifica de la organización
Procedimiento de comunicación con la gerencia	- La que sea especifica de la organización
Elaboración del informe de auditoría	- Identificar los procedimientos para revisión y seguimiento - Identificar procedimientos para evaluar la eficiencia y efectividad operativa - Identificar procedimientos para evaluar controles - Revisar y evaluar la corrección de documentos, políticas y procedimientos

Tabla . Fases de una auditoría típica

Fuente: (ISACA, 2011)

Cada departamento de TI en una organización deberá diseñar o adquirir una metodología, así como los pasos mínimos a seguir en cualquier proceso de auditoría. La documentación de los papeles de trabajo debe contener los planes, programas, actividades, pruebas, hallazgos e incidentes que evidencian una correcta evaluación.

Las mejores prácticas para aplicar sobre los papeles de trabajo requieren que los documentos contengan fechas, estén inicializados, con paginas numeradas, sean relevantes, completos, claros, fáciles de entender, etiquetados debidamente y sean bien custodiados y no necesariamente deben ser impresos. Los documentos de trabajo se consideran el enlace entre los objetivos y el informe final de auditoría que se considera también un papel de trabajo (ISACA, 2011).

De manera general una auditoría deberá seguir una metodología compuesta por fases y es así como es presentada por Sandoval (2012), con base en una auditoría integral. A diferencia

de lo presentado por ISACA (2011), estas fases se estructuran con una fase adicional que, tal y como se muestra a continuación:

Fase I: Análisis general y diagnóstico, está compuesta por actividades a realizar como la evaluación preliminar, plan de trabajo, ejecución y diagnostico.

Fase II: Planeación especifica con actividades como la determinación de objetivos, elaboración de programas de auditoria, determinación de recursos, seguimiento del programa.

Fase III: Ejecución que comprende realizar todas la tareas y actividades establecidas en fase de planeación. De igual forma en esta fase se obtiene la evidencia mediante técnicas y recursos

Fase IV: Informe y resultados donde se incluye las observaciones y oportunidades de mejora con una estructura y presentación adecuada. Puede ser discutida con el cliente donde se definan compromisos y de igual forma se debe presentar en un resumen ejecutivo.

Fase V: En esta fase se presenta un diseño de implementación y evaluación.

Para el cumplimiento acertado de estas fases se recomienda que el equipo auditor este capacitado, sea objetivo, independiente y guarde absoluta confidencialidad. Así mismo el equipo deberá estar familiarizado con el entorno y conocer los controles que serán evaluados y de donde se obtendrá evidencias que constarán en los papeles de trabajo (Sandoval, 2012).

1.4.2.2. Metodología de Evaluación del Desarrollo de los Sistemas

De igual manera otra descripción sencilla de lineamientos metodológicos es la que realiza Echenique (2001), quien indica que en la etapa de desarrollo de sistemas se deberán auditar los programas, su diseño, el lenguaje utilizado, la interconexión entre programas y las características del hardware empleado. Al evaluar un sistema de información se tendrá presente que se debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, así como para reducir la duplicidad de los datos y de reportes para obtener una mayor seguridad de la forma más económica posible.

1.4.2.3. Metodología de Auditoría del Mantenimiento de Software

De acuerdo con lo mencionado por Piattini y del Peso (2007), en la división funcional del departamento de informática de cualquier entidad, una de las áreas que tradicionalmente

aparece es la de desarrollo. En esta área se ejecutan todas las fases que se siguen desde el análisis de los requerimientos para desarrollar un sistema informático, hasta su construcción e implantación. La ingeniería de software de acuerdo con el entendimiento de los autores se describe como el establecer y usar principios de ingeniería fuertes para obtener un software fiable de bajo costo y que cumpla con los requerimientos inicialmente propuestos.

Una auditoría del desarrollo trata de verificar la existencia y aplicación de procedimientos de control, que permita garantizar que el desarrollo de sistemas de información se ha llevado a cabo mediante principios de ingeniería o determinar las deficiencias existentes con base en los mismos principios.(Piattini & del Peso, 2007)

Las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación, en la elaboración del plan estratégico de informática.
- Desarrollo de nuevos sistemas. Es la función principal y la que da sentido al área de desarrollo que incluye para cada uno de los sistemas, el análisis, diseño, construcción e implantación.
- Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. relacionados con el desarrollo. El objetivo es adoptarlos cuando sea necesario.
- Establecimiento de un plan de formación para el personal adscrito al área.
- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Lo siguiente es abordar la auditoría desglosándola en dos grandes apartados metodológicos, como se muestra a continuación.

1. Auditoría de la organización y gestión del área de desarrollo.
2. Auditoría de proyectos de desarrollo de sistemas de información.
    - Aprobación, planificación y gestión del proyecto.
    - Auditoría de la fase de análisis.
    - Análisis de Requisitos del Sistema (ARS).
    - Especificación Funcional del Sistema (EFS).
    - Auditoria de la fase de diseño.
    - Auditoría de la fase de construcción.

_ Auditoría de la fase de implantación.

- Pruebas. Implantación y Aceptación del Sistema (PIA).

En esta sección los autores explican la metodología que se aplica y que es propuesta por la ISACA (Information Systems Audit and Control Association), la misma que basa su desarrollo en la evaluación de riesgos; partiendo de los riesgos potenciales a los que está sometida una actividad. En este caso el desarrollo de un sistema de información determina una serie de objetivos de control que minimicen esos riesgos.

Mencionan también Piatttini y del Peso (2007) que para cada objetivo de control se detallan una o más técnicas de control, que contribuyen a lograr el cumplimiento de dicho objetivo. Además, aportan una serie de pruebas de cumplimiento que permiten comprobar la existencia y aplicación de los controles.

1.4.2.4. Metodología de Auditoría de la Calidad de Software

Siguiendo con la consulta de información relacionada con metodologías de auditoría de software Piattini y del Peso (2007), sostienen que el objetivo de la auditoría de Calidad es descubrir el estado real de los procesos de control de calidad para aportar confianza a dichos procesos.

Entre las razones que se mencionan para realizar una auditoría están:

- Establecer el estado de un proyecto.
- Verificar la capacidad de realizar o continuar un trabajo específico.
- Verificar qué elementos aplicables del programa o Plan de Aseguramiento de la Calidad han sido desarrollados y documentados.
- Verificar la adherencia de esos elementos con el programa o Plan de Aseguramiento de la Calidad.

Como propósito de la auditoría se habla de recoger, examinar y analizar la información necesaria para tomar decisiones de aprobación.

Se contempla bajo este contexto que la auditoría debe tener capacidad para investigar la pericia técnica, el desarrollo del software o la capacidad del departamento de desarrollo, el

esfuerzo disponible, el soporte del mantenimiento o la efectividad de la gestión (Piattini & del Peso, 2007).

1.4.3. Procedimientos para auditar Sistemas informáticos

Auditar Sistemas de Información es un trabajo especializado que requiere de habilidades y el desarrollo de normas para la práctica profesional, como las emitidas por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), aplicables por los miembros de la asociación y por quienes hayan recibido la designación de Auditor Certificado de Sistemas de Información (CISA, por su siglas en ingles), pero de igual manera puede servir para cualquier auditor que cuente con las habilidades necesarias y necesite apoyarse en una normativa específica para realizar auditar un sistema o sistemas de información

ISACA ha implementado estándares que necesitan los requerimientos para la auditoría de sistemas de información y para la generación de informes, de igual forma presenta directrices que se convierten en una guía para aplicar los estándares y por último procedimientos de ejemplo que puede seguir un auditor, al momento de realizar una auditoría. Al mismo tiempo, cuenta con normas profesionales y éticas que debe tener durante su trayectoria como auditor de sistemas informáticos (ISACA, 2011).

Entre los estándares conocidos que cumplen con estas políticas y normas esta COBIT.

1.4.4. COBIT

1.4.4.1. Origen y antecedentes de COBIT

Originalmente se dio a conocer gracias al impulso de Erik Guldentops de origen belga y conocida simplemente como CobiT, Control Objectives for Information and related Technology (Objetivos de Control para la Información y sus Tecnologías afines), registrando su nacimiento en el año de 1996 de la mano de ISACF, Information Systems Audit and Control Foundation (Fundación para el Control y la Auditoría de los Sistemas de Información), la rama investigadora de ISACA, que posteriormente desaparecería a favor de

ITGI, IT Governance Institute (Instituto para el Gobierno de las Tecnologías de la Información), fundado por ISACA en 1998.(García, Palao, & De la Calle, 2016)

Inicialmente se presenta como un catálogo de controles para garantizar la fiabilidad de los Sistemas de Información durante el su ciclo de vida, CobiT evolucionó hasta convertirse en el modelo de referencia para el Gobierno y la Gestión de las TI que es hoy. Su quinta, y última hasta la fecha, edición fue presentada oficialmente por ISACA el día 10 de abril de 2012 (García et al., 2016).

Control Objetives	**CobiT**	**CobiT 2**	**CobiT3**	**CobiT 4/4.1**	**COBIT 5**
Objetivos de Control	Objetivos de Control Marco de Referencia	Directrices de Auditoría Objetivos de Control Marco de Referencia Resumen Ejecutivo	Herramientas de Implementación Directrices de Gestión Directrices de Auditoría Objetivos de Control Marco de Referencia Resumen Ejecutivo	Directrices de Gestión Objetivos de Control Marco de Referencia Resumen Ejecutivo	…..
1983	1996	Abr. 1998	Jul. 2000	Nov. 2005/ Mar. 2007	Abr. 2012

Tabla : Evolución del Modelo COBIT

Fuente: (García et al., 2016)

1.4.4.2. ¿Qué es COBIT?

Es un marco para el gobierno y la gestión de la información y la tecnología (I&T), está dirigido a toda la empresa. La I&T empresarial quiere decir la tecnología y procesamiento de la información utilizada para lograr objetivos de cualquier área, lo que quiere decir, que no se limita solo al departamento de TI.

El marco de referencia COBIT hace una distinción bien diferenciada entre gobierno y gestión, que abarcan varios tipos de actividades, requiriendo distintas estructuras organizacionales con diferentes propósitos.

- **El gobierno** asegura que:
  - Para determinar objetivos empresariales, se evalúan las necesidades, condiciones y opciones de las partes interesadas.
  - A través de la priorización y la toma de decisiones se establece la dirección.
  - En relación con la dirección y los objetivos acordados, se monitorean el desempeño y el cumplimiento.
- **La gerencia** planifica, construye, ejecuta y monitorea actividades en línea con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa (ISACA, 2019).

El marco de referencia de COBIT al ser un conjunto de mejores prácticas permite evaluar la seguridad, eficacia, calidad y eficiencia de los procesos y actividades de TI, así como de las áreas que lo componen para determinar aspectos como los riesgos, gestión efectiva de los recursos, medir el desempeño, cumplimiento de metas y de manera principal medir el nivel de madurez de los procesos de una organización. Busca satisfacer las necesidades relacionadas con los requerimientos del negocio y manejo de la inversión en recursos de TI (Institute IT Governance, 2008).

1.4.4.3. COBIT 4.1

COBIT se basa en tres niveles de actividades de TI para la administración de sus recursos siendo estos niveles los siguientes:

> **Actividades:** Las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.
>
> **Procesos:** Son conjuntos de actividades o tareas con delimitación o cortes de control.
>
> **Dominios:** Es la agrupación natural de procesos denominados frecuentemente como dominios que corresponden a la responsabilidad organizacional (IT Governance Institute, 2007)**.**

1.4.3.4. Marco general de trabajo de COBIT 4.1

Toma como punto de inicio en el ciclo de la información los objetivos del negocio, que deben alinearse con las metas de TI para satisfacer los requerimientos que se generan del negocio agrupados en criterios de información de la siguiente manera:

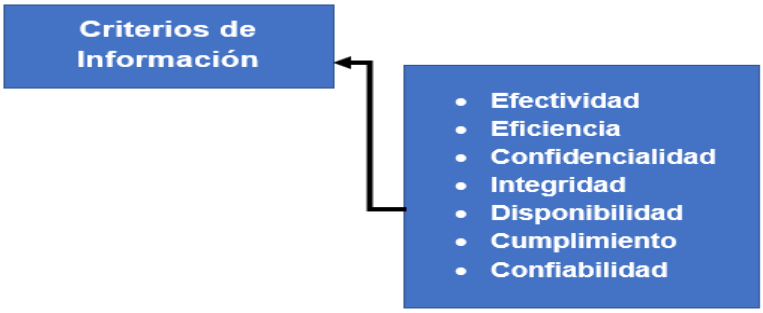


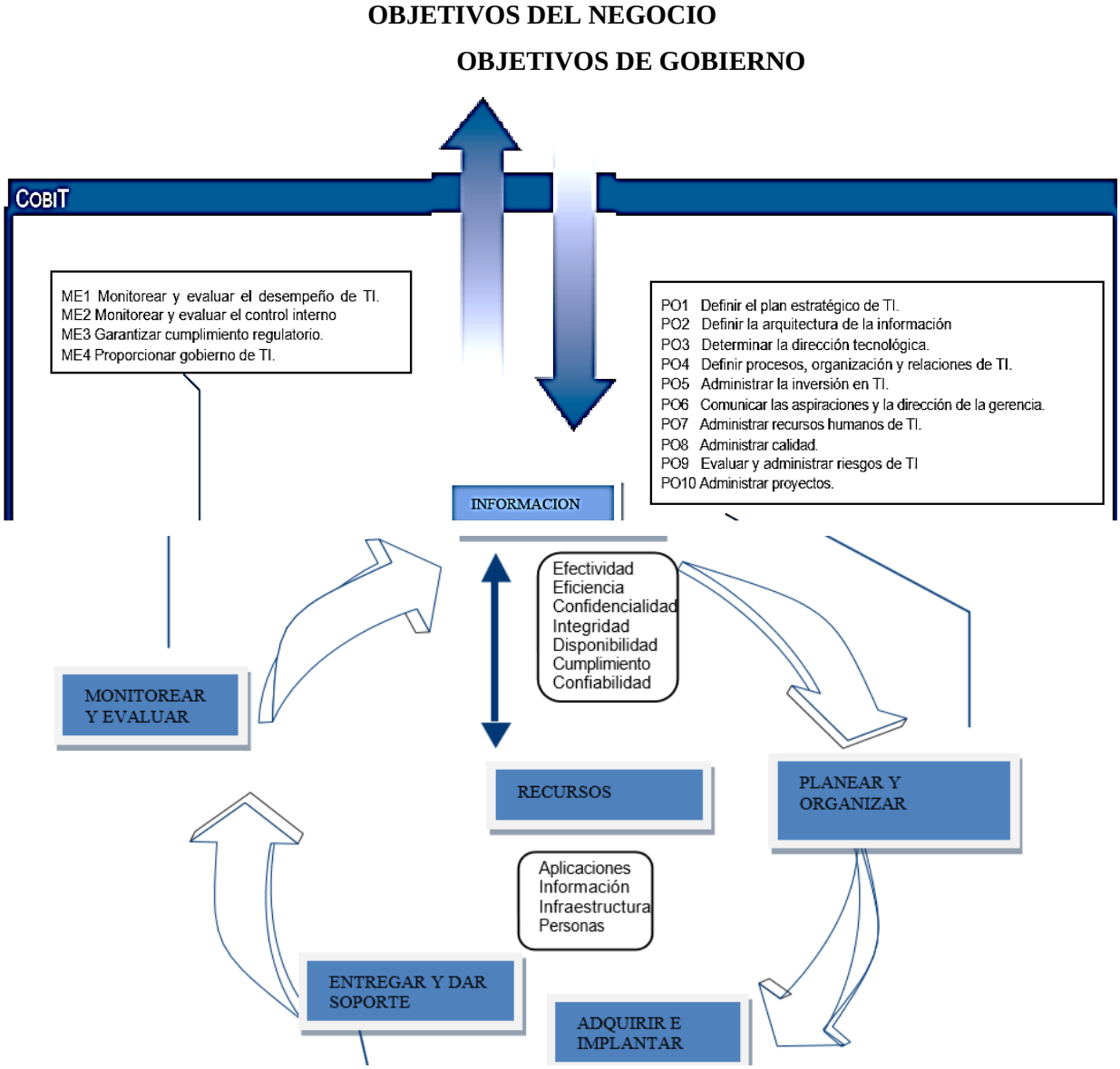
Figura . Criterios de información

Fuente:(IT Governance Institute, 2007)

- **Efectividad:** hace referencia a que la información sea relevante y acertada con los procesos del negocio, y sea entregada de manera oportuna, correcta, consistente y pueda ser utilizada.
- **Eficiencia:** consiste en que la información sea generada optimizando los recursos (más productivo y económico).
- **Confidencialidad:** tiene que ver con la protección de información sensible contra revelación no autorizada.
- **Integridad:** se relaciona íntegramente con la precisión y completitud de la información, así como con su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad:** como la palabra lo indica quiere decir que la información esté disponible cuando sea requerida por los procesos del negocio siempre. Además, corresponde a la protección de los recursos y las capacidades necesarias asociadas.
- **Cumplimiento:** es básicamente el acatar aquellas leyes, reglamentos y acuerdos contractuales, es decir, criterios de negocios impuestos externamente, así como políticas internas.

- **Confiabilidad:** representa proveer la información adecuada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno (IT Governance Institute, 2007).

Las metas de tecnología de información son 28 y deben alinearse a los objetivos del negocio para satisfacer sus requerimientos y se lo podría lograr mediante la ejecución de los procesos de COBIT, compuesto por 4 dominios que sujeta a 34 procesos genéricos, administrando los recursos de TI. Los procesos, también denominados objetivos de control de alto nivel, que a su vez se desglosan en 218 actividades u objetivos de control detallados. En la figura 4 se puede observar los dominios con sus respectivos procesos (IT Governance Institute, 2007).



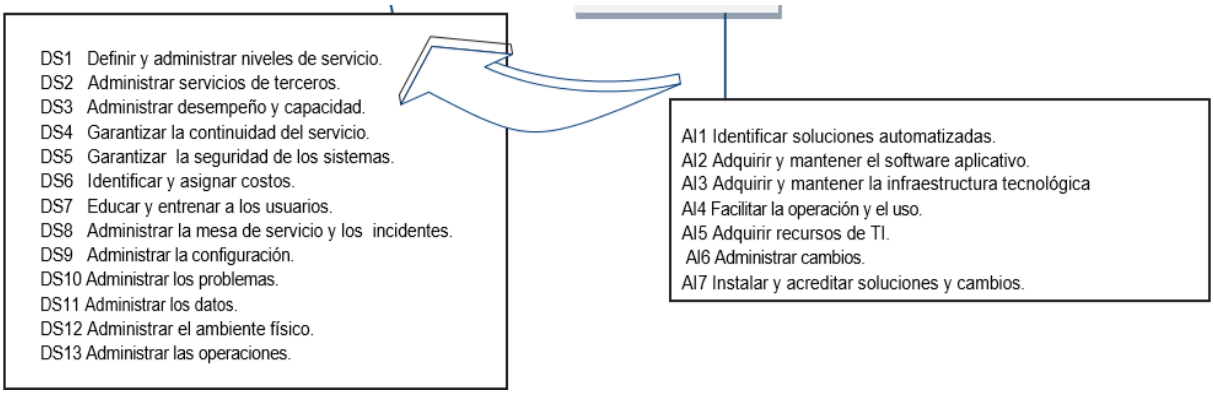


Figura . Marco de trabajo general de COBIT

Fuente: (IT Governance Institute, 2007)

El ejecutar los procesos de modo lógico y estructurado en el área de tecnología de información, permiten implementar el gobierno de TI de manera clara para asegurar una administración integrada y ordenada con la definición de roles, responsabilidades, prácticas de control y métricas para la evaluación de su desempeño y los logros que se puedan obtener en cada uno de los procesos.

COBIT 4.1 especifica que los recursos de información requeridos en toda organización para conseguir las metas de tecnologías de la información son cuatro:

- **Aplicaciones:** Se entiende como los sistemas de información (aplicaciones) que están compuestos por procedimientos manuales y basados en tecnología que proporcionan soporte a los procesos del negocio.
- **Información:** se considera la información interna y externa como, gráficas, sonidos, documentos etc.
- **Infraestructura:** Incluye hardware (equipos), sistemas operativos, sistemas de administración de bases de datos, de redes y de telecomunicaciones, multimedia, etc., e instalaciones.
- **Recurso humano:** Este concepto incluye habilidades, conciencia y productividad del personal para planear, adquirir, prestar servicios, proporcionar soporte y monitorear los sistemas servicios de información.

Estos recursos de información pueden ser requeridos por los objetivos de control de alto nivel (34 procesos), dependerá de cada organización la selección de los que apliquen, balanceando el costo de inversión para su implementación versus lo que implicaría como riesgo no aplicarlo (IT Governance Institute, 2007).

Cada uno de los 34 procesos COBIT 4.1 dispone las siguientes herramientas a ser utilizadas:

Objetivo de control de alto nivel / Proceso de tecnología de información

- Descripción del proceso
- Requerimientos del negocio / criterios de información que soporta
- Prácticas clave para alcanzar el objetivo de control
- Indicadores de medición
- Dominios del Gobierno de TI relacionados con el proceso
- Recursos de TI relacionados
- Actividades del proceso
- Directrices gerenciales (entradas y salidas del proceso)
- Matriz RACI (Responsible, Accountable, Consulted and Informed)
- Metas y métricas (KGI y KPI)
- Modelo de madurez (IT Governance Institute, 2007)

Sin embargo, en el presente trabajo se hará referencia solo a las actividades y a los modelos de madurez de cada proceso descritos a continuación:

- **Actividades del proceso**

  Son objetivos de control que detallan cada una de las actividades de un proceso, y las orienta a obtener un gobierno de tecnología de información efectivo que se consigue además con la evaluación de los riesgos que deben ser administrados en cada proceso.

- **Modelos de madurez**

  Son una derivación del modelo de madurez que el Instituto de Ingeniería de Software (SEI por sus siglas en inglés) definió para la madurez de la capacidad de desarrollo de software. Cobit proporciona un modelo de madurez para cada uno de sus 34 procesos de tecnología de información, en cada uno de los cuales establece una escala como la siguiente:

  1. Inexistente
  2. Ad hoc, inicial
  3. Repetible pero intuitivo
  4. Definido
  5. Administrado y medido
  6. Optimizado

Este modelo de madurez facilitaría a la referencia a ubicar el proceso en la escala con base a una valoración y dependiendo del resultado, involucraría una mejora en el proceso.

La escala de cero a cinco está basada en una escala de madurez simple que indica cómo un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada (IT Governance Institute, 2007).

1.4.5. Calidad como parte del proceso de Ingeniería de Software

1.4.5.1. Ingeniería de Software

De acuerdo con Vega, Rivera y García (2008) sobre la Ingeniería de Software para el establecimiento y Aseguramiento de la Calidad de Software, mencionan que la ingeniería de software es la aplicación práctica de las ciencias computacionales y otras disciplinas mediante el análisis, diseño, construcción y mantenimiento de software y la respectiva documentación asociada. También se indica que es una disciplina tecnológica orientada a generar productos de programación que son desarrollados y modificados dentro de un presupuesto definido, estableciendo que los métodos, procedimientos y herramientas son conjuntados en modelos conocidos como paradigmas existiendo varios como son: cascada, prototipo, costo, espiral, entre otros.

Dentro de la definición de Ingeniería de Software está el ciclo de vida del software que se entiende como el período desde cuando un producto de software es concebido y termina cuando el producto ya no se encuentra disponible para su uso. Se compone de cinco etapas que son: la Planeación, Análisis y Diseño, Codificación, Pruebas, Operación y Mantenimiento.(Vega, Rivera, & García, 2008)

Como parte de la definición de Ingeniería de Software, según Vega et. al. (2008) se encuentra el ciclo de vida del software que se entiende como, el período desde cuando un producto de software es concebido y termina cuando el producto ya no se encuentra disponible para su uso. Se compone de cinco etapas que son: la Planeación, Análisis y Diseño, Codificación, Pruebas, Operación y Mantenimiento.

1.4.5.2. Calidad en el Software

La calidad en el software está en relación directa con el cumplimiento de los requerimientos formulados por el usuario, de tal forma que si un programa no cumple con alguno de estos requerimientos es un software de baja calidad.

Aunque el criterio de cumplimiento de los requerimientos es un factor importante, no es el único, ya que existen condiciones implícitas que el software debe cumplir como son: eficiencia, seguridad, integridad, consistencia, etc.; por lo tanto no se puede afirmar que un software es de alta calidad cuando solo cumple con los requerimientos del usuario.(Bahamon, 1991)

La calidad de software es definida por Pressman (2010), como el proceso eficaz aplicado para crear un producto de software que proporcione a los interesados un valor medible.

La fundamentación de la calidad de software se presenta como factores que tratan de definir características que, si se logran llevar a cabo, pretenden obtener un software de alta calidad.

Los factores de calidad de calidad mencionados por Pressman (2010), establecen características como: confiabilidad, usabilidad, facilidad de dar mantenimiento, funcionalidad y portabilidad como indicadores de la existencia de calidad. No hacen precisamente una medición directa, pero si proporcionan una base aplicable en una medición indirecta mediante una lista de comprobación para evaluar la calidad de un sistema o software desarrollado.

Para Lewis (2010), la calidad de software es vista desde dos perspectivas. La primera es relacionada con el cumplimiento de requerimientos y la segunda es medir la calidad es a través del cliente, quien va a determina si los requerimientos fueron solventados o a su vez son cubiertos, pero sin fallas.

1.4.5.3. Visión general del proceso de prueba de software de siete pasos

Según lo expuesto por Perry (2007), el proceso de prueba de software se basa en la experiencia de más de 1.000 organizaciones de varios países del mundo, afiliadas al Instituto

de Aseguramiento de la Calidad con sede en Estados Unidos. Existen métodos para probar el software y todos pueden llegar a ser efectivos, sin embargo, la experiencia de aplicación en distintas organizaciones hace que sea más aproximado a la realidad.

De manera general según Perry (2007), el proceso de prueba de software está compuesto de siete pasos que siguen el concepto de prueba "V", tal y como se muestra en la figura 9.

El proceso de desarrollo de software y el proceso de prueba de software, en su estructura forman una V, iniciando al mismo tiempo y ejecutándose de forma simultánea hasta el final de un proyecto. El paso final ocurre para los dos procesos (Perry, 2007).

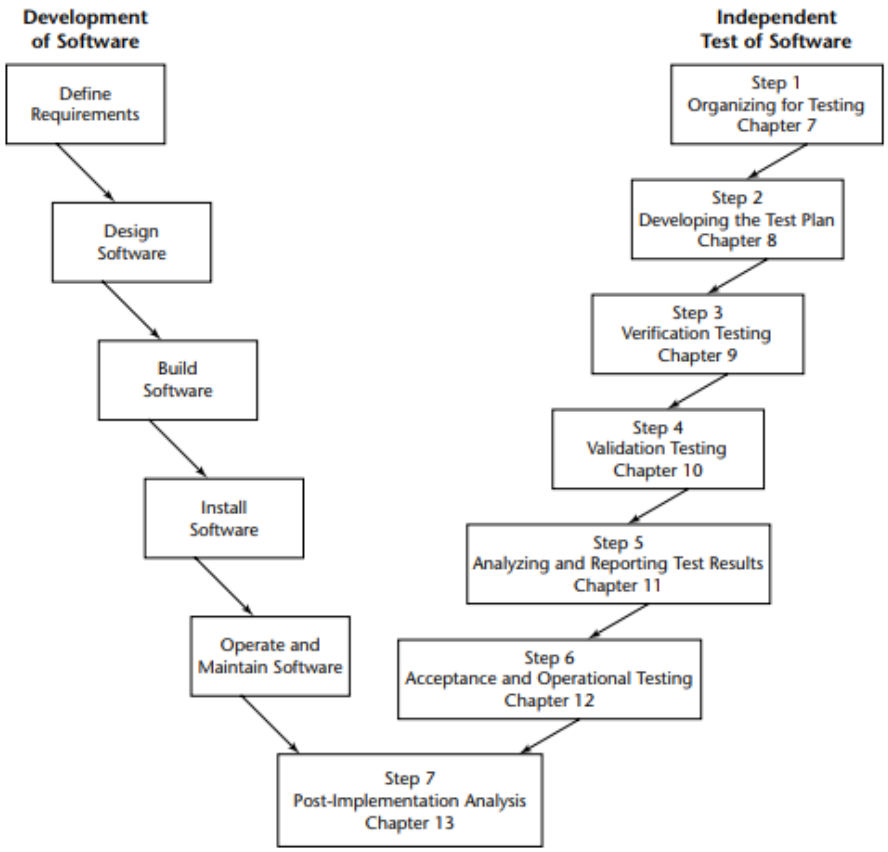


Figura . Siete pasos de proceso de pruebas de software

Fuente: (Perry, 2007)

Para conocer de manera resumida cada uno de los pasos a continuación se muestra una breve descripción:

1. **Organizar para la prueba.**

   a) **Definir el alcance para la prueba. –** como parte de las actividades del paso uno está el determinar qué tipo de prueba se va a realizar.

   b) **Organizar el equipo de prueba.** – se determina en función del tipo de prueba, los posibles participantes.

   c) **Evaluar el plan de desarrollo y estado.** – se considera un requisito previo para la construcción del plan de prueba.

2. **Desarrollo del plan de pruebas.**

   a) **Realizar análisis de riesgo. –** Identificar los riesgos de la prueba

   b) **Escribe el plan de pruebas. -** Se elabora en base al software que se está desarrollando y según la persecución del asociado que está elaborándolo.

3. **Pruebas de verificación.**

   a) **Requisitos de pruebas de software. -** Las fallas pueden presentarse debido a que los requisitos para las pruebas están incompletos o son inconsistentes.

   b) **Diseño de prueba de software.** – Se preocupa por incorporar en el diseño factores internos y externos que se validarán con la ayuda de técnicas. Un buen diseño de las pruebas logrará los objetivos del proyecto**.**

   c) **Software de prueba de construcción. –** Se fundamenta en el método que se elija para construir el software y se trata de realizar la verificación de defectos en la etapa de construcción, a través de pruebas dinámicas durante el paso de validación de pruebas.

4. **Pruebas de validación.**

   a) **Realizar pruebas de validación. –** En este punto se hace referencia a las pruebas unitarias y pruebas del sistema en sus distintas formas.

   b) **Registrar los resultados. –** Documentar los resultados obtenidos.

5. **Análisis y reporte de los resultados de las pruebas.**

   a) **Analizar los resultados de las pruebas. –** Examinar los resultados de las pruebas con el fin de determinar donde se requiere tomar acciones.

   b) **Desarrollar informes de las pruebas. –** El reporte de las pruebas se debe presentar de forma continua. Se lo podría hacer oral y escrito teniendo en cuenta que los defectos e inquietudes deben ser reportados de manera inmediata.

6. **Aceptación y pruebas operativas.**

a) Realizar pruebas de aceptación. – El usuario del software evalúa la aplicabilidad y la usabilidad del software en la ejecución de las funciones diarias, de acuerdo con los requerimientos de software previamente documentados.

b) Probar la instalación del software. - Una vez que el equipo de prueba haya confirmado que el software está listo para la producción, se debe probar la capacidad de ejecutar dicho software en un entorno de producción. Esto prueba la interfaz para operar el software, software relacionado y procedimientos operativos.

c) Prueba de cambios de software. – Aplica para procesos de cambio durante el proceso de implementación y el mantenimiento después de que se implementa el software.

7. Análisis post - implementación. – Las pruebas pueden ser más efectivas si se las hace después de cada tarea de prueba de software. La evaluación, debe involucrar a los desarrolladores, usuarios del software y profesionales de control de calidad si la función existe en la organización de TI.(Perry, 2007)

1.4.5.4. Modelos y Estándares de Calidad del Producto Software

Se toma como referencia el estudio realizado por Moreno, Bolaños, Navia (2010), quienes hacen una exploración de modelos y estándares de calidad del producto de software y los valoran según la disponibilidad, claridad, adaptabilidad, completitud y área de aplicación.

De los modelos expuestos se toman en consideración los de mejor valoración.

Modelo/ Estándar	Descripción	Valoración
MacCall 1977	Este modelo toma en cuenta criterios del desarrollador y del usuario. Divide los factores de calidad en tres aspectos (revisión, transición y operación). Mide la calidad a través de 21 criterios o métricas de calidad y se calcula mediante preguntas de SI o NO constituyendo según el punto de vista de Jorge Moreno, Liliam Bolaños, Manuel Navia subjetividad si es aplicada a muchas personas.	11

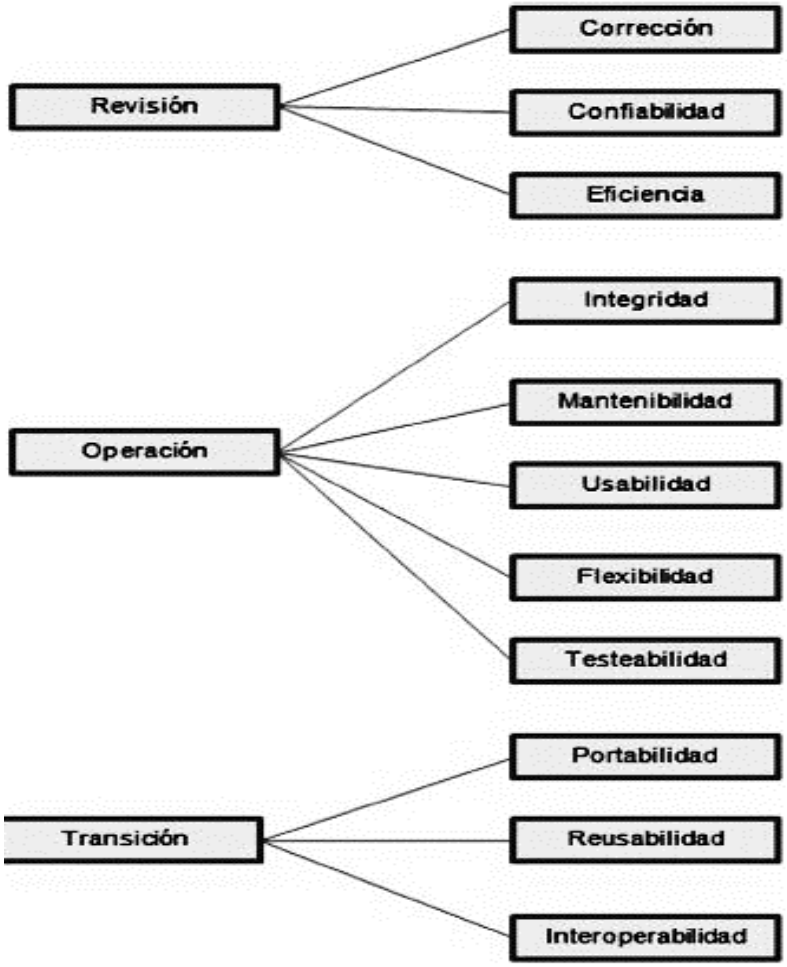


Figura .- Factores de Calidad de McCall

Fuente: (Moreno, Bolaños, & Navia, 2010)

SQAE 1995	Software Quality Assessment Exercise, creado para proveer herramientas y métodos de evaluación que emita un criterio de calidad de software repetible y consistente, que asocie el riesgo relacionado con el área de calidad y genere una lista de riesgos y elementos mitigables que ayuden a seleccionar correctamente desarrolladores de software. Este modelo se basa en modelos como: Boehm, McCall y Dromey, además del estándar ISO/IEC 9126 (desarrollado paralelamente). Las cuatro áreas de calidad con las que SQAE trabaja en cuatro áreas de calidad como: Mantenibilidad, Evolución, Portabilidad y Consistencia, además presenta siete	11

	factores (Independencia, Modularidad, Documentación, Auto descripción, Control anomalía, Diseño simple) para medir la calidad.	

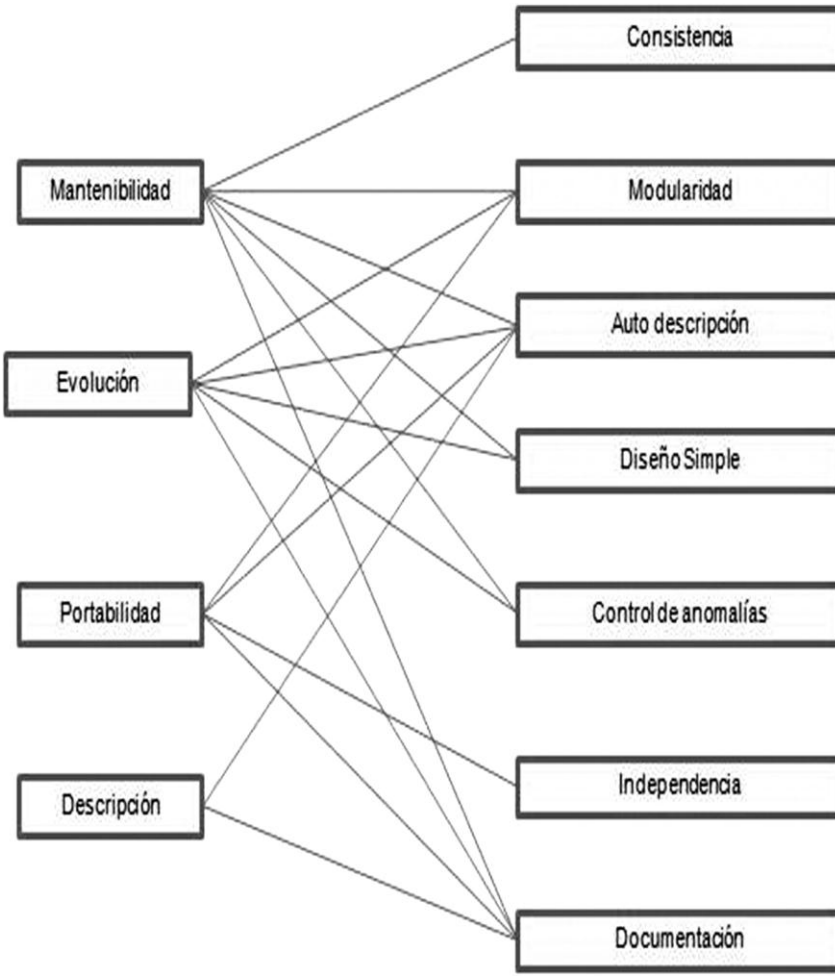


Figura .- Modelo SQAE

Fuente: (Moreno et al., 2010)

Bansiya 1997	Metodología denominada Quality Model for Object-Oriented Design, que desarrolla modelos de calidad de estilo Bottom-up (de abajo hacia arriba), asegurando que los detalles de low-level (bajo nivel) sean bien declarados y computables. Consta de cuatro niveles (L1 a L4) conectados entre sí, contiene 6 atributos de calidad (Reusabilidad, flexibilidad, comprensibilidad, funcionalidad, extensibilidad y efectividad) y 11 propiedades de diseño que complementan a los atributos. Además, posee una serie de métricas para la evaluación de	11

	estos.	
ISO 9126 (1991/2001)	El estándar ISO 9126 presenta dos partes, el Modelo de calidad para calidad externa e interna, y el Modelo de calidad para calidad en uso. La primera parte, seis características de calidad externa, divididas en sub-características que representan la calidad interna con influencia sobre las características externas. La segunda parte, presenta cuatro características de calidad, a ser validadas por el usuario.	11

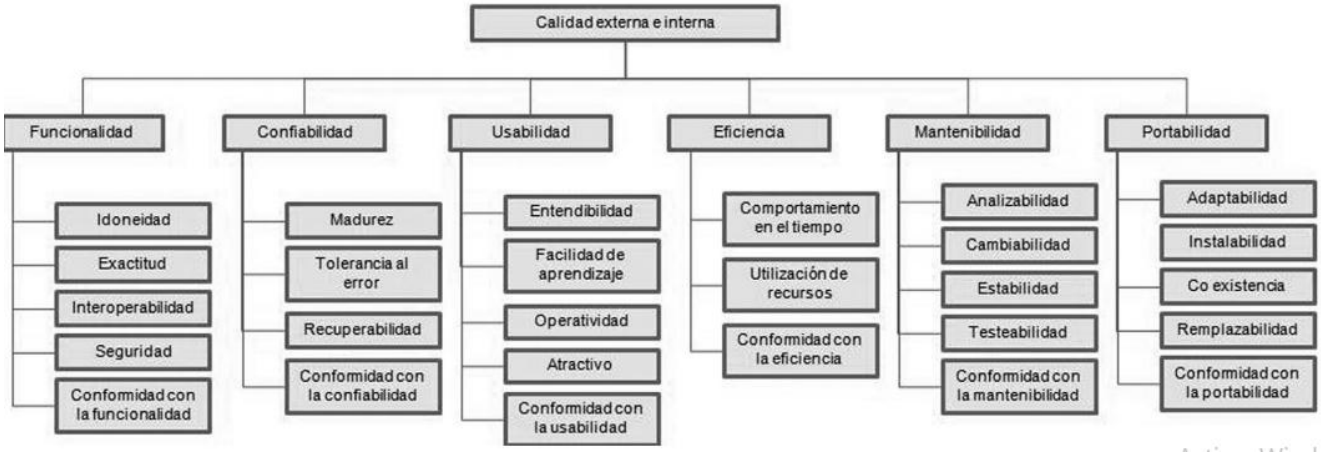


Figura .- Modelo de Calidad Interna y Externa

Fuente: (Moreno et al., 2010)

FURPS 1987	El nombre del modelo hace relación a cinco categorías que se refieren a: Funcionalidad (Functionality), Usabilidad (Usability), Confiabilidad (Reliability), Desempeño (Performance) y Soportabilidad (Supportability), de ahí su nombre. Su estructura es la siguiente:	10

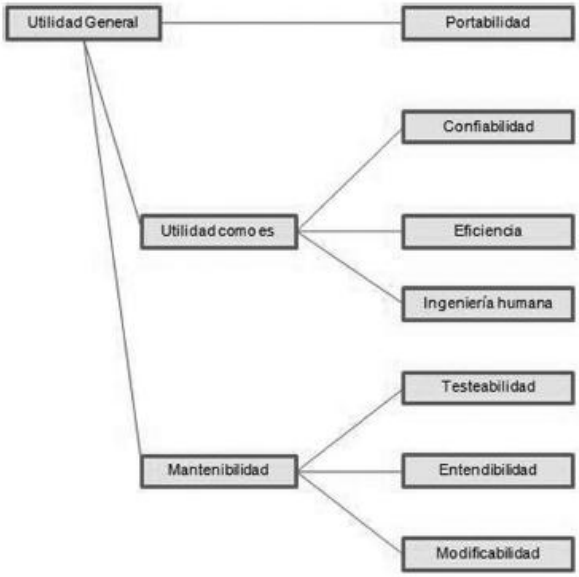


Figura .- Factores de calidad FURPS

Fuente: (Moreno et al., 2010)

QUINT2 -2002	Denominado modelo de calidad de software ISO extendido, que se presenta como un conjunto más grande del grupo de características y sub-características del modelo ISO 9126. Las sub-características se derivan de cada una de las de las características. Su estructura es la siguiente:

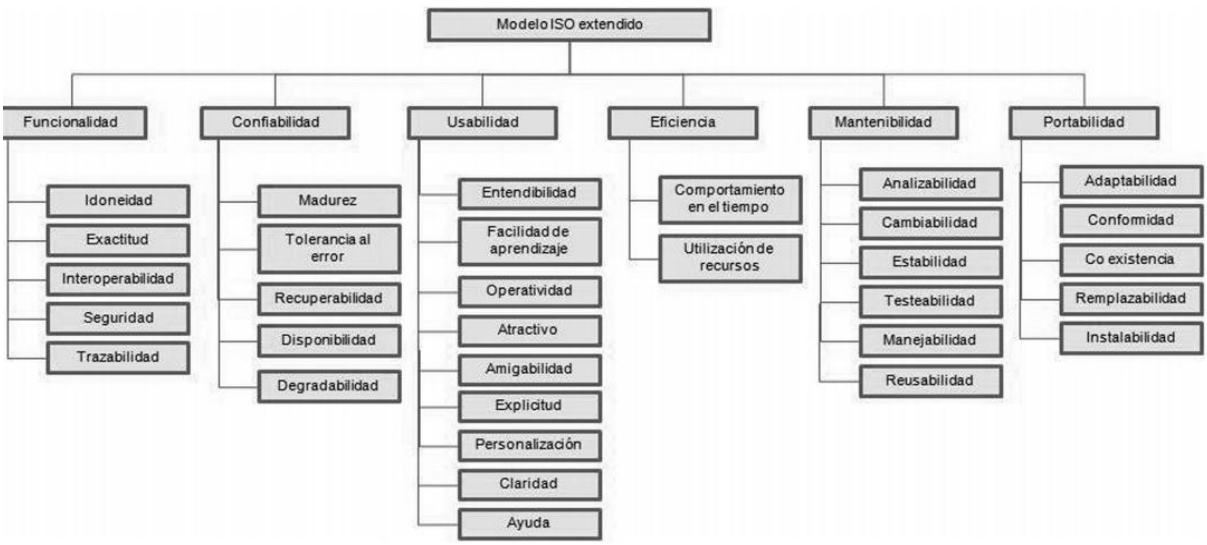


Figura .- Características y sub - características de QUINT2

Fuente: (Moreno et al., 2010)

Tabla .- Modelos y Estándares de Calidad de software

Fuente: Autor

Los modelos revisados en la tabla resumen, cubre varios aspectos de calidad de software en general, los que se presentan con mayor valoración son un referente y tiene como fin dar a conocer elementos relevantes, que permitan fundamentar un criterio unificado sobre la calidad. Cada modelo plantea una perspectiva de calidad que se relacionan entre sí, con el objetivo de generar un producto de software de calidad, con atributos medibles ya sea cualitativa o cuantitativamente y que cómo resultado sea el cumplimiento de las expectativas de calidad.

CAPÍTULO II

ESTADO DEL ARTE

La auditoría informática es un tema que ha ido cambiando en el tiempo, ha sido empleada cuando se ha requerido conocer el estado de los procesos informáticos. Como parte de esta evolución también se han incorporado nuevos procesos que pueden ser auditados, como es el caso de los que se ejecutan en el área que busca obtener software de calidad.

De acuerdo con el estudio realizado por Hernández y Lomprey (2008) sobre la importancia de la calidad en el desarrollo de software, donde se menciona que los fallos de software afectan a todos los sectores y a todos los países con un alto impacto no solo en pérdidas económicas si no en la satisfacción de los clientes. En el mismo estudio se identifica una de las causas por las que los sistemas fallan y que está relacionada directamente con el proceso de calidad, siendo esta, él no contar con tiempo suficiente para las pruebas debido a que se inician al final de los proyectos, cuando ya existen retrasos. Este antecedente se complementa con otros que en este estudio se refieran como a la procedencia de los problemas de software:

Motivo	**Porcentaje**
Requerimientos no comprendidos	50%
Diseño no comprendido o incorrectamente trasladado de los requerimientos	30%
Codificación (error de programación o diseño mal comprendido):	20%
Personal técnico y directores de software con formación deficiente en control de calidad	50% y 70% respectivamente

Tabla . Procedencia de los problemas en la calidad de software

Fuente: Hernández y Lomprey (2008)

Aspectos como el de realizar un buen análisis de calidad desde el inicio del desarrollo de software, puede ahorrar recursos económicos a las organizaciones ya que al detectar un defecto en una etapa inicial de definición de requerimientos, demandará poco tiempo para su corrección, mientras que, si es detectado en la fase de producción, requerirá de al menos 100 horas para lograr corregirlo (Hernández & Lomprey, 2008).

Otro aspecto importante para considerar es poder detectar fallas en el proceso que se sigue para determinar la calidad de un producto de software. El proceso para la certificación de un sistema o producto de software también requiere una evaluación e identificación de factores que pueden estar obstaculizando su mejora, sobre todo en pequeñas y medianas organizaciones de desarrollo de software. Es de este tema que trata el estudio presentado por García, Amescua, y Velasco (2006), quienes dan a conocer 10 factores que impiden la correcta aplicación de prácticas eficientes de verificación y validación de software.

Estos factores se enumeran de la siguiente manera:

- **Factor 1:** que trata de acerca de los modelos de referencia (ISO 12207, CMMI, IEE1074 entre otros) con definiciones de las prácticas de verificación y validación que no son entendibles ni fáciles de usar.
- **Factor 2:** relacionado con los mismos modelos de referencia, que no proporcionan un enlace coherente entre los procesos de verificación y validación y resto de los procesos de ingeniería necesarios para desarrollar software.
- **Factor 3**: conocer por parte de la gerencia cual será el retorno de la inversión que se realice. Se necesita estimar los costos de un programa de mejora en los procesos.
- **Factor 4:** es posible que el costo de mejorar los procesos que se siguen para verificación y validación de software sean altos y no se pueda realizar en pequeñas y medianas organizaciones.
- **Factor 5:** se necesita conocer la situación actual de los procesos de verificación y validación (incluye las pruebas que se realizan al software) y en algunas organizaciones se piensa que es una pérdida de tiempo y recursos.
- **Factor 6:** la mejora de las actividades de pruebas con la inclusión de herramientas para la automatización supone mejoras en el proceso de pruebas, pero limita las capacidades del conjunto de procesos que son parte de la validación.

- **Factor 7:** las revisiones técnicas por pares de los productos de análisis y diseño producen un costo extra y sobrecarga de trabajo que las organizaciones no pueden asumir.
- **Factor 8:** la definición detallada de los casos de prueba de sistema, se considera una tarea burocrática que requiere mucho esfuerzo, sin un beneficio claro porque en muchas de las ocasiones la persona que escribe los casos es quien ejecuta la prueba.
- **Factor 9:** una de las principales dificultades para la correcta ejecución de los procesos de certificación o validación de software, es el desconocimiento de los usuarios para realizar la revisión de un análisis o diseño, así como para realizar una prueba de un módulo o componente de software.
- **Factor 10:** los retrasos en los desarrollos hacen que la dirección opte por recortar los tiempos de pruebas, asumiendo los costos asociados y los riesgos que implica la realización de un mantenimiento correctivo posterior a la implementación. Este problema aparte de ser un impacto negativo para cualquier organización, también desmotiva al personal de la organización(J. García et al., 2006).

La problemática en los procesos que se siguen para el desarrollo y la evaluación del producto de software, expuesta por Hernández y Lomprey (2008) y Garcia et al.(2006) inciden en su correcta aplicación de un modelo de calidad, tal y como lo describen Rodríguez y Piattini (2015), en una investigación que recopila estudios sobre certificación de la calidad del producto de software, donde se destaca la necesidad de incluir las características del producto en la certificación, adoptar un nuevo modelo de acuerdo a lo que propone la familia ISO/IEC 2500, diferenciar la evaluación de la certificación ya que ésta se la debe realizar de acuerdo a un estándar internacional y por último la importancia de tener un entorno tecnológico que automatice las actividades.

Esta investigación extrae los requisitos para llevar a cabo la evaluación y certificación de la calidad del producto software, que además de contar con personal de experiencia, se pueden llevar a cabo de acuerdo con los siguientes elementos: un modelo de calidad, un proceso de evaluación y un entorno tecnológico que de soporte a los dos elementos anteriores.(Rodríguez & Piattini, 2015)

El modelo de calidad define las características del producto software (funcionalidad que tiene un producto, la usabilidad, la seguridad o la mantenibilidad del producto software) que

deberá ser parte del proceso de evaluación, de acuerdo con el desglose al más bajo nivel de las características que derivan en indicadores medibles. Para el modelo de calidad también es importante definir umbrales que reflejen el valor de la calidad, siendo la razón para no utilizar la familia de normas ISO/IEC 25000, ya que no determina indicadores, métricas o umbrales que ayuden a las organizaciones, al momento de evaluar el proceso para la obtención de calidad en un producto de software y que esté acorde con lo requerido.

En la investigación que presentan Rodríguez y Piattini (2015), existe un proceso de evaluación de las actividades a realizar para determinar la calidad de un producto de software, descritas como un conjunto de partes del proceso de verificación de la calidad, que incluyen el código fuente, los requisitos, los modelos, los casos de prueba, el producto en ejecución, entre otros aspectos a evaluar. Además, agregan los pasos que el evaluador debe seguir, así como las herramientas y el personal que apoyará, hasta llegar a obtener los hallazgos que se remitirán en un informe de resultados.

Un producto de software puede ser desarrollado bajo requerimientos de cualquier organización y para diferentes propósitos; de manera general estos pueden ser sistemas para bancos, para la educación, para la salud, la construcción, etc. Al estar enfocada esta investigación a presentar una metodología para auditar los procesos del área de calidad de software en entidades bancarias, se realiza la búsqueda de estudios afines con el tema propuesto, siendo poca la información obtenida, sin embargo, se analizan los temas que más relación tenían.

En el entorno de evaluación o auditoría del proceso de software, se encuentra una metodología planteada por Suárez (2009), quien establece una herramienta de evaluación que está basada en prácticas efectivas del Modelo de Madurez y Capacidad Integrado para el Desarrollo (CMMI-DEV v1.2), orientada a pequeñas y medianas empresas de software que desean mejorar sus procesos y de manera especial el que se sigue para generar software de calidad. En este estudio se realiza un mapeo entre las causas detectadas del fracaso con las áreas o fases del proceso de Nivel 2 de CMMI-DEV v1.2, que daría la opción de adaptación para cada organización pequeña y mediano tamaño; acogiendo la idea del mapeo de los procesos del área de calidad, con las partes que corresponden a COBIT.

De igual manera se tomó como referencia de este estudio, la estructura de niveles que el modelo entrega para identificar el estado de los procesos de software, posicionados de

acuerdo con las áreas claves de cada uno de ellos, con el fin de definir su madurez de acuerdo con CMMI. Además, se considera como ayuda la implementación de cuestionarios con preguntas orientadas a evaluar la gestión de los proyectos como parte del ciclo de vida del software y los procesos que se ejecutan en el área de calidad de software.

Otro punto importante que se tomó como aporte de este estudio, es el diseño que se utiliza para la obtención de los datos, con cuestionarios de preguntas cerradas y respuestas que se rigen a la frecuencia (Siempre, Usualmente, A veces, Rara vez y Nunca) y verificación (No sé y No Aplica) de la aplicación, utilización y ejecución de las distintas actividades realizadas en los procesos (Suárez, 2009).

El estudio que relaciona temas de auditoría de la calidad con un sistema informático es el que propone Dragomir (2017) en Bucharest Rumania, quien da a conocer una metodología de auditoría para el control de calidad en el dominio de TI, distribuida por etapas que además se compone de características y factores que describen las actividades que se ejecutan a lo largo de una auditoría. Se enfoca en el control del sistema de calidad de los nuevos productos generados para ser parte de un entorno tecnológico. Las etapas que en esta investigación se mencionan, son un aporte importante para el desarrollo de la metodología que se propone en este trabajo ya que muestran una estructura que marca un inicio, un fin y sus características y factores son fácilmente entendibles.

En resumen, las etapas planteadas por Dragomir (2017) son las que se muestran el cuadro siguiente:

ETAPAS	CARACTERÍSTICAS	FACTORES
Inicio de la auditoría	- Establecer los objetivos y criterios - El impacto que va a tener la auditoría - Conformar el equipo auditor - Iniciar el proceso de auditoría en un lugar determinado	- Personalizar con las especificaciones de la empresa - Aceptar los objetivos identificados - Comunicar los requisitos relacionados - Métodos de proyección de productos y hechos que los influyen

		- Tecnología utilizada para la producción de componentes de TI - Comunicar los contenidos del proceso de auditoría - Evitar situaciones de incompatibilidad. - Notificar sobre el inicio del procedimiento de auditoría
Análisis de documentos	- Solicitar los documentos que reflejan la calidad de los productos de TI - Disponer de los documentos que reflejan la situación real -Determinar las conformidades de la mejor manera	- Analizar las conformidades de la documentación - Establecer las competencias del personal involucrado en la actividad de control de calidad - Se verifican los documentos, decisiones de cada nivel jerárquico - Recolectar los documentos específicos relacionados con tareas y responsabilidades - Analizar los documentos del sistema de control de calidad - Presentar las listas centralizadas con objetos auditables - Evaluar los riesgos y el control interno
Preparación para la auditoría específica en un cierto lugar	- Planificar detalladamente la auditoría - Asignar tareas al equipo de auditoría - Fijar los documentos de trabajo	- Recopilar datos de entrada para la planificación de la auditoría (información general sobre la compañía, su actividad específica, su página web, el segmento de mercado identificado, la capacidad de la compañía de hardware y software, informes de auditoría, planes para desarrollar y probar

		productos de TI) - Planificar la auditoría (visibilidad de todas las actividades, tipos de proyectos, métodos para producir componentes de TI y su control de calidad; examen detallado si el auditor jefe lo solicita para obtener mejores resultados) - Establecer técnicas de auditoría
Actividades de auditoría específicas del lugar	- Sesión abierta de la actividad de auditoría - Verificar la información confrontando los registros - Opinión del auditor - Comunicar a los beneficiarios - Sesión final	- Realizar entrevistas con los decisores y los ejecutantes, documentos, examen a la calidad de los productos - La auditoría de las herramientas para generar productos de TI se realiza a través de tres técnicas: • Elección de una muestra de productos y seguimiento de su evolución desde la proyección hasta la entrega, verificando la exactitud de todas las etapas • La segunda técnica es la vía inversa, desde la entrega hasta la proyección. Aquí se analizan las salidas en todos los niveles • La auditoría de cada fase de proyección para varios proyectos implementados - Las observaciones de auditoría con base en pruebas recopiladas que se reflejan en el

		incumplimiento del proceso de control de calidad. Las fuentes para obtener las pruebas pertinentes son: informes de auditoría anteriores, reclamación del beneficiario, grabaciones de calidad, documentos, fallas remediales, acciones correctivas previas, observación de la actividad durante el proceso de auditoría, entrevistas con los empleados involucrados en actividades de calidad
Informe de los resultados de la auditoría	- Conformidad del sistema de control de calidad - Eficiencia en la implementación del sistema de control de calidad - Capacidad de asegurar un sistema de control de calidad eficazmente	- Nivel de conocimiento de los empleados involucrados en el proceso de producción y sistema de control de calidad - El modo de cumplimiento de las tareas individuales y colectivas - Grado de conformidad de la actividad - Exactitud de documentos - Personal calificado de la empresa
Fin de la auditoría	- Notificar acerca del sistema de control de calidad administrable - Sensibilizar a los beneficiarios sobre el impacto de las medidas correctivas.	- Material de presentación - Equipo de auditoría - Conclusiones parciales y finales del proceso de auditoría - Reunión presidida por el auditor principal - Alcance de la auditoría (asegurar el control de calidad de los productos de TI) - Resumen del informe de auditoría

		- Gráficos del proceso de auditoría - Límites de auditoría - Presentación de incumplimientos y también la forma en que esto afecta el sistema de control de calidad - Un auditor puede admitir que puede haber un incumplimiento no descubierto - Informe de firma y conclusión
Después del enfoque de auditoría	- Incumplimiento - No se resuelve el Incumplimiento - No se corrige el Incumplimiento	- El incumplimiento de los productos de TI del sistema de control de calidad, está especificado por la norma ISO 9001/2008. El auditor jefe los presenta. Estos pueden ser vistos como observaciones mayores o menores y simples - Todos estos deben ser presentados en los informes de auditoría y firmados por el beneficiario. El papel del auditor es proponer al beneficiario la siguiente auditoría

Tabla .- Resumen de las etapas que presenta la Metodología para el control del sistema de calidad

Fuente: (Dragomir, 2017)

Las fases de la auditoría que propone Dragomir (2017), son planteadas de otra manera de acuerdo con lo expuesto por Castro y Álvarez (2018) en su trabajo de tesis realizado en Bogotá Colombia y cuyo tema es el diseño de una metodología de auditoría para el control de los procesos de pruebas en entidades financieras. Este trabajo utiliza como base ITIL V3,

específicamente el proceso de Gestión de Cambios, ayudando a que se realice e implemente adecuadamente todos los cambios en la infraestructura y servicios de TI.

Con base en el proceso de ITIL V3, se preparan una serie de actividades que forman parte de tres objetivos principales que son: planificar, analizar y evaluar los cambios que se efectúan en un sistema. Entre las actividades se encuentra la que hace referencia a la evaluación de los cambios desarrollados en un sistema, realizando una medición a través de indicadores de rendimiento y cumplimiento del proceso, revisión post implementación para conocer si los cambios efectuados fueron exitosos (Castro & Alvarez, 2018).

El haber planteado en este proyecto de tesis el desarrollo de una metodología de auditoría basada en el Marco de Referencia COBIT, es importante conocer cómo actúa este marco en los procesos de auditoría de los sistemas. En la investigación realizada por Santacruz, Vega, Pinos y Cárdenas (2017) en el país, dan a conocer la ayuda que brinda el sistema COBIT, ya sea como un modelo o como una guía al momento de realizar auditorías de sistemas de información y tecnología de una organización, mediante una conceptualización resumida de términos claves para su comprensión.

El valor óptimo de la tecnología de la información en las organizaciones es un propósito planteado por el sistema COBIT. Además, la versatilidad que brinda al ser un modelo que puede ser utilizado en diferentes tipos de organizaciones, sin importar su tamaño, ya sea pública o privada hace que cada vez existan más interesados en su estudio, aplicación y sea empleado en todo el mundo por quienes están a cargo de los procesos tecnológicos y de negocio. Basa su esquema en cinco principios y siete habilitadores. En el caso de COBIT 5 al ser un ejemplo de mejores prácticas utiliza la gestión y el gobierno para describir las acciones.(Santacruz, Vega, Pinos, & Cárdenas, 2017)

Principios	Habitadores	Procesos
1. Satisfacer las necesidades del accionista. 2. Considerar la empresa de punta a punta. 3. Aplicar un único	1. Principios, políticas y modelos de referencia. 2. Procesos. 3. Estructuras organizacionales. 4. Cultura, ética y	Modelo general de procesos compuesto por cuatro dominios: - Planificar y Organizar (PO). - Adquirir e

modelo de referencia integrado. 4. Posibilitar un enfoque holístico. 5. Separar gobierno de la gestión. 6. Habilitadores	comportamiento. 5. Información. 6. Servicios, infraestructura y aplicaciones. 7. Gente, habilidades y competencias.	Implementar (AI). - Proveer y Soportar (DS) - Monitorear y Evaluar (ME).

Tabla .- Principios, habilitadores y procesos de COBIT
Fuente: (Santacruz et al., 2017)

Esta investigación menciona a COBIT como un sistema que ayuda a realizar auditorías informáticas, se conceptualizan los temas relacionados con el gobierno y gestión de TI indicando que:

El gobierno evalúa las necesidades de los accionistas para asegurar que los objetivos empresariales se cumplan. Establece la toma de decisiones, así como el monitoreo del desempeño, cumplimiento y el progreso comparado con la dirección y objetivos acordados (EDM, por Evaluar, Dirigir, Monitorear).

Por su parte la gestión se encarga de planificar, construir, ejecutar y monitorear actividades dispuestas por la dirección para el cumplimiento de objetivos empresariales (PBRM o Planificar, Construir, Ejecutar y Monitorear).(Santacruz et al., 2017)

Lo expuesto por Santacruz et al. (2017), permitió entender de mejor manera de qué forma se desarrollaron metodologías que utilizan COBIT para realizar sus auditorías, como es el caso del proyecto realizado por Coronel (2013), quien plantea la evaluación al Gobierno de TI enfocándose en gran parte de su trabajo en los riesgos y las seguridades, a través del conocimiento de normas y elementos de COBIT 5. También realiza un análisis comparativo de los requerimientos de COBIT 5, la Normativa de la Superintendencia de Bancos y Seguros (SBS) y el estándar ISO/IEC 27005 con el fin de asignarles un peso diferenciado en la evaluación del Gobierno, Riesgos y Cumplimiento de TI, a aquellos puntos comunes encontrados que constituyen elementos de cumplimiento obligatorio. Incluye un mapeo de los requerimientos de la norma de Gestión del Riesgo Operativo de la SBS y las mejores

prácticas de COBIT 5, obteniendo datos donde se muestra que la mayor cantidad de requerimientos normativos se enfocan en controles de seguridad de la información y que en algunos casos coincide con los procesos de COBIT 5 que se seleccionan para la evaluación del Gobierno, Riesgos y Cumplimiento de TI, en una institución financiera.

De igual manera, realiza un mapeo de los requerimientos de la norma de Medidas de Seguridad de la SBS, frente a las prácticas clave de COBIT 5 y el estándar ISO/IEC 27005. Realiza 62 comparaciones con los procesos, entre los cuales destacan la gestión de controles de procesos de negocio, administración de operaciones, y de seguridades. Se obtiene como resultado cinco procesos que coinciden con los que se seleccionan para la evaluación del Gobierno, Riesgos y Cumplimiento de TI en una institución financiera, y cuatro coinciden con los mapeados en la norma de Riesgo Operativo.

Se menciona por parte de Coronel (2013a), que COBIT 5 establece distinciones entre gobierno y gestión, englobando diferentes tipos de estructuras organizacionales que se encaminan a diferentes propósitos. Esto implica que no todos los elementos y herramientas que provee COBIT 5 apoyan de la misma manera al Gobierno corporativo de la organización, por lo que la metodología que se propuso utilizó solo aquellos procesos que contribuyen de manera directa a proveer información y soporte al cuerpo de gobierno de TI de las entidades evaluadas.

Otro tema similar donde se utiliza COBIT para realizar una auditoría, es el planteado por Garcia y Chiclote (2016) en la ciudad de Trujillo Perú, quienes proponen un modelo de evaluación que en este caso es al proceso de mantenimiento de sistemas de información de una entidad financiera basado en COBIT. Este trabajo muestra de manera sencilla como relacionar los dominios de COBIT con los procesos del área de mantenimiento de sistemas, para que posteriormente sean utilizados en la ejecución de una auditoría. Esta selección formula un modelo de evaluación que se compone de los procesos, actividades que se ejecutan en el área, así como los dominios de COBIT y guías de referencia para la utilización del modelo, tomando estas prácticas como aporte para el desarrollo de la metodología propuesta en este trabajo de tesis.(L. García & Chiclote, 2016)

Los trabajos investigados representan un apoyo y ayuda, ya que en cada una de las propuestas existen iniciativas que son tomadas en cuenta para el desarrollo de este trabajo de tesis, utilizando de la mejor manera los argumentos propuestos en cada uno de ellos para

acoplarlos, de tal manera que se pueda generar una metodología de auditoría informática al área de calidad de software que solvente en parte la problemática existente.

En lo que respecta al modelo empelado como base se identifica las buenas prácticas que ofrece el Marco de Referencia COBIT y que se utiliza en varias metodologías que se crearon para realizar auditorías de TI en entidades financieras. Emplear COBIT va en concordancia con lo dispuesto de manera general por la Superintendencia de Bancos (2010), en su artículo 20 específicamente en lo que respecta a las Normas para la calificación de los auditores internos de las entidades sujetas a control de la SBS donde se menciona como recomendación tomar en consideración las directrices de auditoría previstas por ISACA.(Superintedencia de Bancos, 2010).

CAPÍTULO III

DISEÑO DE LA METODOLOGÍA

3.1. Campo en el que se puede aplicar la metodología propuesta

Como está planteado en este trabajo de tesis, la metodología de auditoría que se propone se encaminada a ser aplicada en el sector financiero, específicamente para entidades de mediano tamaño en el país. Según un reporte de la Superintendencia de Bancos (2018), existen nueve bancos privados que están en el rango de medianos y son a los que potencialmente les podrían interesar aplicar la metodología desarrollada cuando se requiera de una auditoría en el área de calidad de software.(Superintedencia de Bancos Portal Estadístico, 2018)

Al ser para las entidades financieras de mediano tamaño a donde está dirigida la metodología de auditoría y particularmente para el área de calidad de software, es importante conocer la estructura organizacional que presentan por lo menos dos de ellas, para así ubicar el área de Calidad de Software dentro de dicha estructura. Se toma como referencia dos de las nueve entidades financieras clasificadas como medianas en Ecuador y se explica que una de las razones para su elección es la facilidad que se tuvo para obtener información, sin embargo, no se puede dar a conocer su nombre por temas de confidencialidad para lo que de aquí en adelante se denominaran banco A y banco B para su identificación.

3.2. Área de Calidad de Software del Banco A

El Banco A está formado por varias Gerencias Nacionales que reportan directamente a la Presidencia Ejecutiva y a un Directorio. Estas Gerencias a su vez distribuyen actividades a otras Gerencias como la Gerencia de Tecnología, en donde se encuentra la Gerencia denominada Diseño y Entrega del Servicio.

En esta gerencia existe entre otras, la Sub Gerencia de Calidad y es aquí donde se ejecutan los procesos para emitir las certificaciones a los mantenimientos y nuevos desarrollos tecnológicos. Está representada por un Sub Gerente, que su vez coordina las actividades que serán ejecutadas por los Técnicos de Calidad a través de Gestores y Especialistas de Calidad, según la necesidad de cada proyecto.

A continuación, se muestra el organigrama del Banco A, donde se puede identificar el área de Calidad representada por la Subgerencia de Calidad:

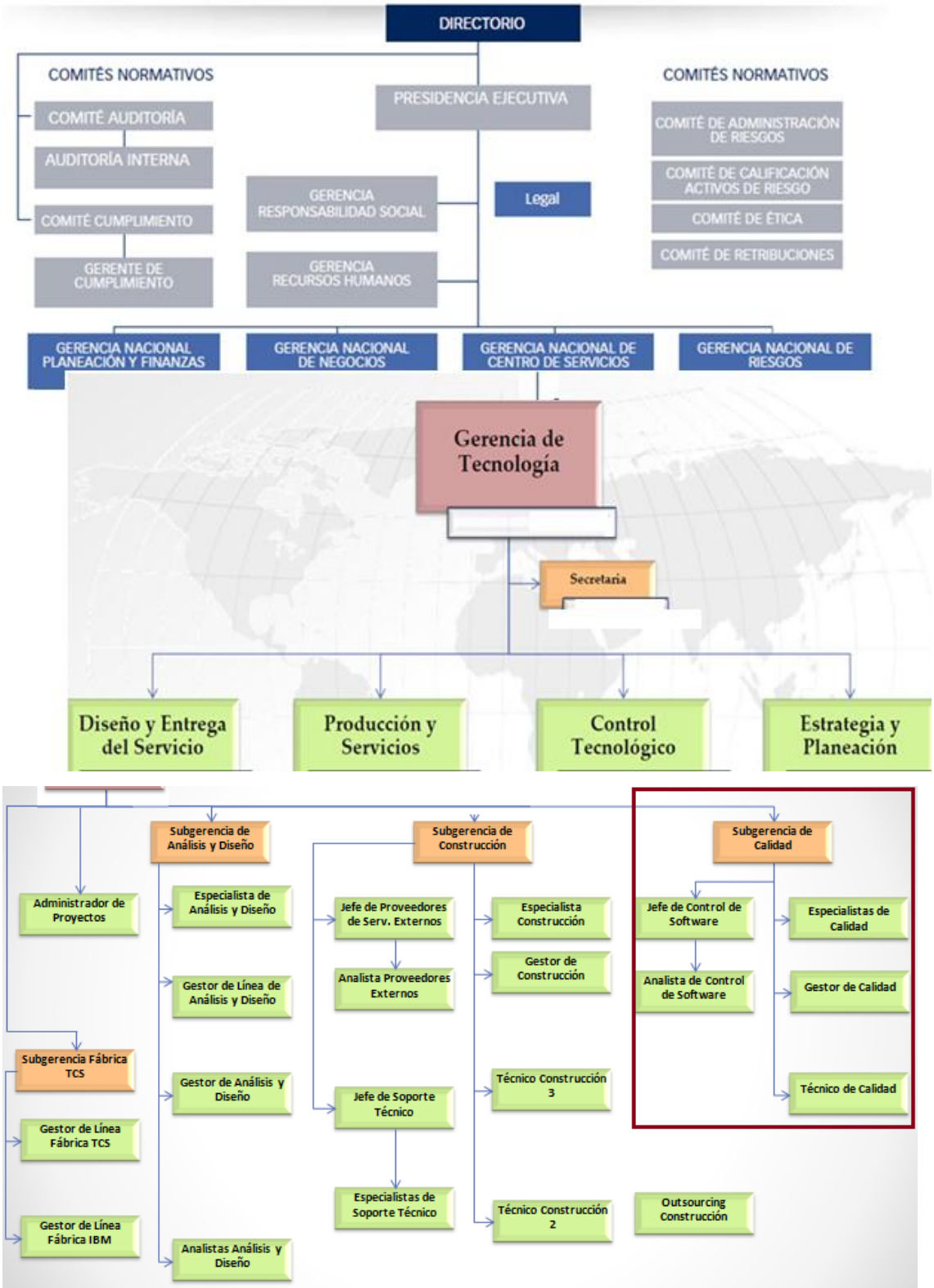


Figura 10.- Estructura organizacional del Banco A (Área de Calidad)

Fuente: Autor

3.2.1. Procesos del Área de Calidad de Software del Banco A

De acuerdo con la información obtenida mediante una entrevista realizada a una colaboradora cuyo nombre es Alexandra García, gestora del Área de Calidad de Software del Banco A, quien da a conocer que los procesos de calidad de un producto de software suelen dividirse en pruebas estáticas y dinámicas. Donde las pruebas estáticas se centran en evaluar la calidad de la documentación generada como entregables, realizando revisiones repetidas, mientras que las pruebas dinámicas, hacen referencia a la ejecución de las pruebas del software a fin de medir la calidad y el nivel de cumplimiento según los requerimientos.

A continuación, se mencionan los procesos que se ejecutan en cada etapa durante el ciclo de pruebas en el área de Calidad del Banco A (A. Garcia, comunicación personal, 5 de noviembre del 2018).

Proceso General	**Etapas del proceso de pruebas en el Área de Calidad**	**Actividades de cada etapa**
	Estimación y Análisis Pruebas	- Hacer el análisis y completar la documentación necesaria - Revisar y aprobar Análisis - Realizar ajustes - Revisar y aprobar Análisis - Recibir aprobación de análisis y actualiza avance - Subir documentación al sistema. - Cambiar Etapa - Planeación de pruebas

Administrar la Calidad	Planeación de Pruebas	- Generar casos de prueba preliminares - Generar set de datos - Revisar documentación - Realizar ajustes - Recibir retroalimentación del script de pruebas - Actualizar avance, documentación y subir a la herramienta - Comunica a Gestor de construcción - Cambiar etapa del requerimiento en el sistema
	Ejecutar pruebas y seguimiento de incidentes	- Ejecutar las tareas prerrequisitos para las pruebas - Ejecutar los casos de pruebas. - Generar documento de pruebas positivas - Ingresar defecto / generar matriz de incidencias - Enviar matriz de incidencias a construcción - Realizar el seguimiento de las fechas de solución - Recibir respuesta de construcción - Actualizar la matriz de eventos con las respuestas dadas. - Elaborar Informe Final de Pruebas - Generar Manuales de Usuario y Actividades Funcionales para la Implementación

Tabla .- Etapas del proceso de pruebas en el área de Calidad del Banco A

Fuente: (A. Garcia, comunicación personal, 5 de noviembre del 2018)

Bajo este esquema se identifica un solo proceso denominado Administrar la Calidad del cual se derivan subprocesos, que son en sí, las etapas de ciclo de pruebas o lo que puede ser la metodología de pruebas que este banco utiliza para llegar a certificar sus soluciones.

3.3. Área de Calidad de Software del Banco B

El Banco B en su organigrama general presenta diferentes áreas creadas para cumplir con los objetivos y estrategias planteadas. A continuación, en la figura siguiente se detalla la estructura:

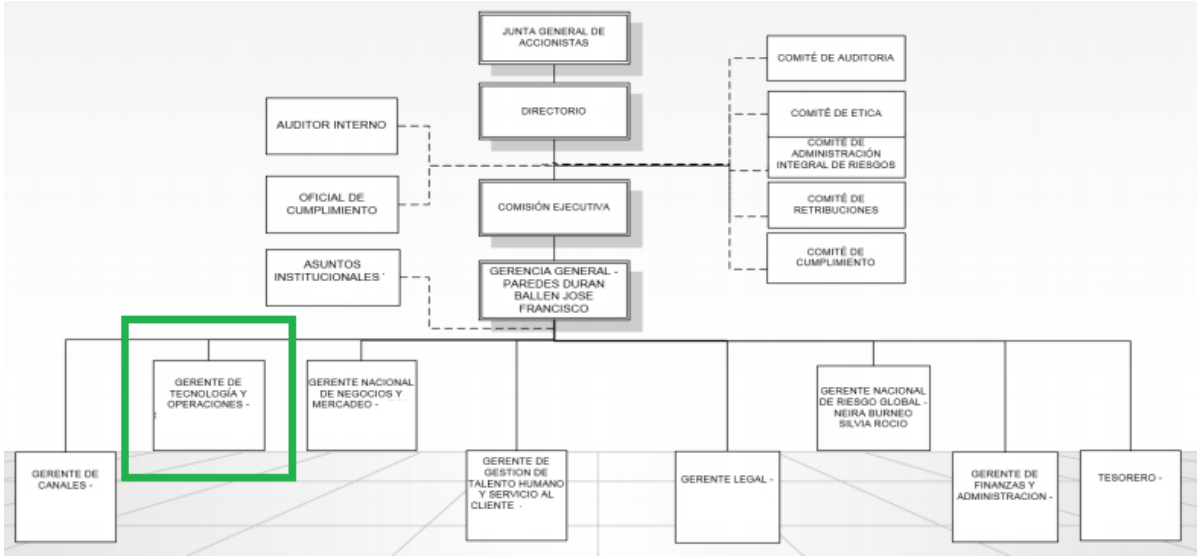


Figura .- Estructura Organizacional del Banco B

Fuente: Autor

Dentro del organigrama, el Banco B presenta varias Gerencias entre la que se encuentra la Gerencia de Tecnología y Gestión BPO, que incluye la Sub Gerencia de GTO y la Sub Gerencia de TI.

El esquema que maneja el Banco B, es la exteriorización de los procesos operativos y tecnológicos, en alianza estratégica con una empresa que brinda entre otros, el servicio para la ejecución de los procesos de desarrollo y certificación de software debiendo ser supervisados por representantes de la Gerencia de Tecnología y Operaciones para llevar un control de dichos procesos (Cabrera, 2014).

3.3.1. Procesos del Área de Calidad de Software del Banco B

Debido al antecedente acerca del esquema operativo y tecnológico con el que se maneja el Banco B y dada la necesidad de conocer las fases que se ejecutan y bajo qué modelo metodológico de desarrollo trabajan en la mayoría de los proyectos de esta empresa que brinda servicios al banco, se contactó a un colaborador de dicha empresa, que forma parte del área de Control de Calidad de Software. Alejandro Ushca ayudó con información general de las fases que se siguen en el proceso de certificación de un desarrollo para los proyectos que se generan como requerimientos del Banco B (A. Ushca, comunicación personal, 20 de septiembre del 2018).

Fases del ciclo de pruebas	**Objetivos de cada fase**	**Actividades de cada fase**
Fase1	Análisis de Requerimientos.	- Estimación de Esfuerzo del PRY
Fase 2	Diseño de Alto y Bajo Nivel	- Generar Estrategia de Pruebas - Analizar la aplicación de escenarios de Prueba - Generar Escenarios de Prueba -Determinar Colaterales - Gestionar revisión y aprobación de Estrategia
Fase 3	Construcción	- Generar guiones de prueba - Gestionar la revisión y aprobación de guiones - Subir guiones a la herramienta

Fase 4	Pruebas de Integración	- Receptar y revisar guiones - Preparar data para ejecución de pruebas - Ejecutar casos de prueba - Validar resultados - Registrar, reportar, seguir y validar solución de novedades a través de la herramienta - Registrar respaldo de pruebas ejecutadas. - Soporte a usuarios expertos durante la ejecución de las pruebas - Registrar, reportar, seguir y validar solución de novedades a través de la herramienta - Preparar informe de certificación final
Fase 5	Paquete y liberación	- Pruebas inspección final - Participación en Comité de cambios
Fase 6	Post Implementación	- Soporte estabilización (Pruebas funcionales)

Tabla .- Fases del ciclo de pruebas que ejecuta el proveedor de servicios del Banco B
Fuente: (A. Ushca, comunicación personal, 20 de septiembre del 2018)

Las fases y actividades que se incluyen en el ciclo de vida del proyecto están íntegramente ligadas al proceso de Control de Calidad que lleva a cabo la empresa externa que da el servicio al Banco B, siendo esta empresa la encargada de velar por el correcto funcionamiento de los sistemas, una vez implantados en producción.

Al estar el proceso de desarrollo y certificación de software fuera del entorno del banco, se hace necesario mantener una constaste evaluación para saber cómo se está llevando a cabo, que tan eficiente es el trabajo realizado e incluso evidenciar si se debería mantener o no el servicio externo. Esto se podría determinar mediante una auditoría a los procesos de calidad,

con la ayuda de una metodología específica que valore cada etapa durante el proceso de certificación de los desarrollos tecnológicos.

3.3. Relación de los componentes de COBIT con los procesos de Calidad

El Marco de referencia COBIT, a través de sus componentes ofrece soporte a las diferentes necesidades de control de TI, ayudando a la gerencia a cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. Además, permite el desarrollo de políticas claras y de buenas prácticas para el control de TI por parte de las organizaciones.

Los procesos de TI al tener la posibilidad de relacionarlos con procesos específicos de diferentes áreas, como lo es el área de Calidad de Software, están sujetos a ser evaluados mediante objetivos de control que generan como resultados indicadores de desempeño, madurez, eficiencia y efectividad en una organización.

3.3.1. Selección de los dominios y procesos de COBIT que fundamentan la metodología de auditoría desarrollada

Los procesos de TI fundamentan sus actividades en un modelo genérico de cuatro dominios que son: planear y organizar, adquirir e implementar, dar soporte y monitorear y evaluar; siendo estos equiparados con las áreas de TI donde se planea, construye, ejecuta y monitorea.

Al ser el objetivo general de este trabajo el desarrollo de una de la metodología de auditoría a un área específica de TI, que realiza el Control de la Calidad de Software ya sea implementado o adquirido, se hace necesario evidenciar que dominios proporcionan una guía que evalúen esta meta que forma parte de los objetivos de TI.

Los procesos y actividades contenidos por esta meta fueron identificados en la etapa de análisis de los procesos y actividades que se ejecutan en las áreas de Calidad de Software de dos bancos medianos en Ecuador.

Para tener una idea clara del dominio, los procesos (principales y secundarios) y prácticas de gestión seleccionados para evaluar la Calidad de Software, se elabora la siguiente tabla, donde se realiza un mapeo entre las metas relacionadas con TI y los procesos de TI que proporciona COBIT.

COBIT			**Meta relacionada con TI:**
Dominio:	**Proceso:**	**Objetivo de control:**	**Procesos del área de calidad de software en entidades financieras medianas en Ecuador**
Planear y organizar.	PO4 Definir los procesos, organización y relaciones de TI.	PO4.7 Responsabilidad de aseguramiento de calidad de TI.	Organigrama del área, roles y responsabilidades de sus integrantes.
	PO8 Administrar la calidad.	PO8.1 Sistema de administración de calidad.	Se mantiene un proceso genérico de administración de la calidad de los servicios prestados por TI y para el caso de estudio, específicamente para el área de Calidad de Software.
		PO8.2 Estándares y prácticas de calidad.	Se incluye en la ejecución de los procesos del área metodologías, mejores prácticas, estándares, procedimientos y políticas claras de calidad.
		PO8.6 Medición, monitoreo y revisión de la calidad.	El monitoreo y revisión interno y externo constante del desempeño y mejora continua del cumplimiento de los procesos, se reflejará en un registro de la información que se usará para aplicar medidas

			correctivas.
Adquirir e implementar.	AI2 Adquirir y dar mantenimiento a software aplicativo.	AI2.8 Aseguramiento de la calidad del software.	Se cubre las expectativas del negocio a través de requerimientos que son realizados en su totalidad en el menor tiempo, con un bajo costo y sin reproceso por problemas que se puedan generar en producción.
	AI7 Instalar y acreditar soluciones y cambios.	AI7.2 Plan de prueba.	Establecer un plan de pruebas que contemple todas las etapas del proceso de certificación y que se ajuste a la metodología de pruebas utilizada, con una definición clara de roles y responsabilidades. Debe incluir los requerimientos de pruebas más relevantes como desempeño estrés, usabilidad y seguridad.
		AI7.4 Ambiente de prueba.	Mantener un ambiente para pruebas dedicado, con datos de prueba relevantes y que se asemeje en su infraestructura (hardware, software y arquitectura) con el ambiente de producción.
		AI7.6 Prueba de cambios.	Plan preestablecido para el manejo de incidentes que garantice la trazabilidad. Mantener un archivo de lecciones aprendidas. Las

		actividades ejecutadas deben respaldarse con pistas de auditoría.
	AI7.7 Prueba final de aceptación.	Garantizar una evaluación formal de todos los posibles escenarios de prueba, así como la interacción con los componentes del sistema (hardware, software, y procedimientos de tecnología). Los resultados deben ser documentados y aprobados por un responsable.

Tabla .- Mapeo de dominios, procesos y objetivos de control relacionados la calidad de software

Fuente: Autor

De acuerdo con el mapeo de los procesos y actividades de calidad identificados como parte de los procesos de calidad de software de entidades financieras medianas en Ecuador, se deduce que existen varios dominios que contribuyen a la estrategia de TI que cubre el desarrollo, implementación e integración de soluciones de TI con los procesos del negocio.

Mediante la definición de los procesos, el detalle de los objetivos de control y la relación con la meta de TI (Calidad de Software), se busca esclarecer cuestionamientos de la gerencia que revelen si los proyectos generan soluciones satisfactorias, son entregados a tiempo, están dentro del presupuesto, son de calidad y no afectan a las operaciones actuales del negocio.

Además, se toma como guía el trabajo realizado por Coronel (2013), quien plantea una metodología para evaluar al Gobierno de TI en instituciones del Sistema Financiero ecuatoriano. Este trabajo presenta un enfoque orientado a la evaluación del Gobierno de TI, mediante un flujo ordenado, compuesto por etapas o fases y que además hace énfasis su apoyo en los procesos y dominios de COBIT.

3.3.2. Modelo de evaluación basado en COBIT que establece la Metodología desarrollada

Como resultado del análisis anterior, el modelo de evaluación desarrollado basado en COBIT, se compone de dos dominios y cuatro procesos que utilizan nueve prácticas de gestión u objetivos de control; que se constituyen en la base modelo para la evaluación efectiva de cada proceso que ejecuta actividades en el área de Calidad de Software en entidades bancarias medianas en Ecuador.

	Objetivos de control
1.	PO4.7 Responsabilidad de aseguramiento de calidad de T
2.	PO8.1 Sistema de administración de calidad
3.	PO8.2 Estándares y prácticas de calidad
4.	PO8.6 Medición, monitoreo y revisión de la calidad
5.	AI2.8 Aseguramiento de la calidad del software
6.	AI7.2 Plan de prueba
7.	AI7.4 Ambiente de prueba
8.	AI7.6 Prueba de cambios
9.	AI7.7 Prueba final de aceptación

Tabla .- Modelo de evaluación que se plantea en la metodología desarrollada

Fuente: (IT Governance Institute, 2007)

3.3.3. Formulario de referencia para evaluación según el modelo

Cada objetivo de control hace parte de un proceso y este a su vez de un dominio como se muestra en la tabla 8. Para un mejor entendimiento del modelo, se genera una guía de referencia establecida mediante un formulario que incluye información sobre: el objetivo de cada proceso del área, sus actividades, la relación con los objetivos de control o denominadas también prácticas de gestión y las metas con sus respectivas métricas.

PROCESO:	Definir los procesos, organización y relaciones de TI
OBJETIVO DEL PROCESO:	Dar a conocer a los dueños de los procesos, las tareas y responsabilidades por parte de la dirección del área de

	Calidad de Software, para lograr el correcto funcionamiento de los servicios. La segregación de funciones está dentro de lo previsto por parte de la dirección para evitar que una sola persona esté a cargo de todos los procesos; además busca dar a conocer cuanto conocimiento y experiencia tiene cada persona mediante evaluaciones periódicas.

META DE ACTIVIDADES	MÉTRICAS RELACIONADAS
- Definir un marco de trabajo de procesos para TI. - Establecer organismos y estructuras organizacionales apropiadas.	- % de roles con puestos documentados y descripciones de autoridad. - % de funciones / procesos operativos de TI que se conectan con las estructuras operativas del negocio. - Frecuencia de reuniones de los comités estratégicos y de dirección.

META DEL PROCESO	MÉTRICAS RELACIONADAS
- Establecer estructuras y relaciones organizacionales para TI, que sean flexibles y responsables. - Definir propietarios, roles y responsabilidades de forma clara para todos los procesos TI y para todas las relaciones con los interesados.	- # de responsabilidades conflictivas en vista de la segregación de funciones. - # de escalamientos o problemas sin resolver debido a la carencia o insuficiencia de asignaciones de responsabilidad. - % de *stakeholders* satisfechos con el nivel de respuesta de TI.

METAS DE TI	MÉTRICAS RELACIONADAS
- Responder a los requisitos de gobierno de acuerdo con las directivas del consejo directivo. - Responder a los requisitos de negocio de acuerdo con la estrategia del negocio Crear la agilidad de TI.	- Satisfacción de participantes (encuestas). - # de iniciativas de negocio retrasadas debido a la inercia operativa de TI o a la falta de disponibilidad de las capacidades necesarias. - # de procesos de negocio que no reciben soporte por parte de TI que lo deberían

	recibir de acuerdo con la estrategia. - # de actividades esenciales de TI fuera de TI que no están aprobadas o que no están sujetas a los estándares de TI.

PRÁCTICA DE GESTIÓN RELACIONADA
PO4.7Responsabilidad de aseguramiento de calidad de TI Asignar al grupo de aseguramiento de calidad la responsabilidad para el desempeño de sus funciones, proporcionando controles y la práctica para comunicarlos. La ubicación organizacional y las responsabilidades y tamaño del grupo de aseguramiento de calidad satisfacen los requerimientos de la organización.

Tabla .- Formulario de referencia para PO4 Definir los procesos, organización y relaciones de TI

Fuente: Elaborado por el autor (IT Governance Institute, 2007)

PROCESO:	PO8 Administrar la calidad
OBJETIVO DEL PROCESO:	Elaborar y mantener un sistema de administración de calidad, con procesos, estándares y un plan de calidad, que debe promover la mejora continua. Las responsabilidades del aseguramiento de la calidad determinarán realizar actividades como revisiones de auditoría que ayudan a cumplir los objetivos del plan. Se evidenciará el uso de metodologías durante el ciclo de pruebas, así como la documentación de las pruebas, los programas utilizados y los reportes generados.
META DE ACTIVIDADES	**MÉTRICAS RELACIONADAS**
- Definir estándares y prácticas de calidad. - Monitorear y revisar el desempeño interno y externo contra los estándares	- % de proyectos que reciben revisiones de QA. - % de personal de TI que recibe entrenamiento administrativo /

y prácticas de calidad definidos.	concientización. - % de proyectos y procesos de TI con participación en el aseguramiento de calidad por parte de los participantes. - % de procesos que reciben revisiones de QA Porcentaje de interesados que participan en encuestas de calidad.
META DEL PROCESO	**MÉTRICAS RELACIONADAS**
- Establecer estándares y cultura de calidad para los procesos de TI. - Establecer una función de aseguramiento de la calidad para una TI eficiente y efectiva. - Monitorear la efectividad de los procesos y proyectos de TI.	- % de defectos no descubiertos antes de entrar en producción. - % de reducción en el número de incidentes de alta severidad por usuario por mes. - % de proyectos de TI revisados y autorizados por QA que satisfacen las metas y objetivos de calidad. - % de procesos de TI revisados de manera formal por QA de manera periódica que cumplen las metas y objetivos de calidad.
METAS DE TI	**MÉTRICAS RELACIONADAS**
- Garantizar la satisfacción de los usuarios finales con oferta de servicios y niveles de servicio. - Reducir los defectos y repeticiones de trabajo en la prestación de servicios y soluciones. - Entregar proyectos a tiempo y dentro del presupuesto, satisfaciendo estándares de calidad.	- % de interesados satisfechos con la calidad de TI (ponderado por importancia).
PRÁCTICADE GESTIÓN RELACIONADA	
PO8.1 Sistema de administración de calidad Establecer y mantener un QMS estandarizado, formal y continuo, con respecto a la administración de la calidad, alineado con los requerimientos del negocio. El QMS	

identifica los requerimientos y los criterios de calidad, los procesos claves de TI y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo con los criterios y políticas y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.
PO8.2 Estándares y prácticas de calidad Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI orientando a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia para mejorar y adaptar las prácticas de calidad de la organización.
PO8.6 Medición, monitoreo y revisión de la calidad Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

Tabla .- Formulario de referencia para PO8 Administrar la calidad

(IT Governance Institute, 2007)

Fuente: Autor

PROCESO:	AI2 adquirir y dar mantenimiento a software aplicativo
OBJETIVO DEL PROCESO:	Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Para ello se debe realizar un correcto análisis de los requerimientos de usuario, las pruebas funcionales deben abarcar la mayor cantidad de escenarios y deben estar de acuerdo con el plan de pruebas y los estándares establecidos. La documentación generada del proceso de ejecución de pruebas debe ser clara y para el caso del material de consulta para usuarios, debe cubrir la mayoría de las inquietudes que pueden surgir.
META DE ACTIVIDADES	**MÉTRICAS RELACIONADAS**

- Traducir los requerimientos del negocio a las especificaciones de diseño. - Adherirse a los estándares de desarrollo para todas las modificaciones. - Priorizar los requerimientos con base en la relevancia del negocio. - Separar actividades de desarrollo, pruebas y operación. - Aprovechar la inversión en tecnología existente.	- % de proyectos de software aplicativo con plan de aseguramiento de calidad del software desarrollado y ejecutado. - % de proyectos de software aplicativo con revisión y aprobación adecuadas de la conformidad con los estándares de desarrollo. - Tiempo promedio de entrega de la funcionalidad, con base en las medidas como puntos funcionales o líneas de código.
META DEL PROCESO	**MÉTRICAS RELACIONADAS**
- Adquirir y mantener aplicaciones que satisfagan en forma rentable los requerimientos definidos para el negocio. - Adquirir y mantener aplicaciones de acuerdo con la estrategia y la arquitectura de TI. - Garantizar que el proceso de desarrollo sea oportuno y rentable.	- % de proyectos de desarrollo a tiempo y dentro del presupuesto. - % del esfuerzo de desarrollo que se gasta en mantenimiento de las aplicaciones existentes - # de problemas de producción por aplicación que provocan tiempo perdido notorio - Defectos que se reportan por mes (por punto funcional).
METAS DE TI	**MÉTRICAS RELACIONADAS**
- Definir cómo los requerimientos funcionales y de control del negocio, se traducen a soluciones automatizadas efectivas y eficientes. - Adquirir y mantener sistemas de aplicación integrados y estandarizados.	- % de proyectos que entregan los cambios en el negocio dentro del marco de tiempo requerido. - # de proyectos donde no se alcanzaron los beneficios establecidos debido al deficiente diseño o desarrollo de la aplicación. - % de usuarios satisfechos con la funcionalidad entregada.
PRÁCTICA DE GESTIÓN RELACIONADA	

AI2.8 Aseguramiento de la calidad del software
Desarrollar e implantar los recursos, ejecutar un plan de aseguramiento de calidad del software para obtener la calidad que se especifica en la definición de los requerimientos, políticas y procedimientos de calidad de la organización. Los asuntos para considerar en el plan de aseguramiento de calidad incluyen especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas.
AI2.9 Administración de los requerimientos de aplicaciones
Garantizar que, durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

Tabla .- Formulario de referencia para AI2 Adquirir y dar mantenimiento a software aplicativo (IT Governance Institute, 2007)

Fuente: Autor

PROCESO:	AI7 Instalar y acreditar soluciones y cambios
OBJETIVO DEL PROCESO:	La verificación y confirmación de que la solución cumple con los requerimientos propuestos, son el resultado haber realizado correctamente las pruebas con las especificaciones de cambios, desempeño, aceptación final y operacional de acuerdo con los estándares utilizados. El seguimiento es el complemento para determinar si la solución implementada proporciona los beneficios esperados y no se generan observaciones.
META DE ACTIVIDADES	**MÉTRICAS RELACIONADAS**
- Establecer una metodología de prueba que garantice pruebas de aceptación suficientes antes de liberar. - Rastrear cambios a todos los componentes de la configuración. - Realizarla planeación de la	- Grado de involucramiento del *stakeholder* en el proceso de instalación y acreditación. - % de proyectos con plan de prueba documentado y aprobado. - # dé lecciones aprendidas de la revisión posterior a la implantación.

liberación. - Ejecutar y aprobar los resultados de las pruebas por parte de la administración del negocio.	- % de errores encontrados durante la revisión de aseguramiento de calidad en las funciones de instalación y acreditación. - # de cambios sin las autorizaciones requeridas de la gerencia antes de la implantación
META DEL PROCESO	**MÉTRICAS RELACIONADAS**
- Verificar y confirmar que las aplicaciones y soluciones de tecnología se ajustan al propósito deseado. - Liberar y distribuir apropiadamente las aplicaciones aprobadas y las soluciones de tecnología. - Preparar a los usuarios y operadores del negocio para el uso de aplicaciones y soluciones de tecnología. - Garantizar que las nuevas aplicaciones de negocio y los cambios a las aplicaciones existentes estén libres de error.	- # de errores encontrados durante auditorías internas o externas con respecto al proceso de instalación y acreditación. - Repetición del trabajo después de la implantación debido a pruebas inadecuadas de aceptación. - Llamadas de usuarios debido a entrenamiento inadecuado. - Tiempo perdido de aplicación o reparaciones de datos provocadas por pruebas inadecuadas.
METAS DE TI	**MÉTRICAS RELACIONADAS**
- Garantizar que las transacciones automatizadas de negocio y los intercambios de información sean confiables. - Reducir los defectos y revisiones de trabajo en la entrega de soluciones y servicios. - Responder a los requerimientos de acuerdo con la estrategia de negocio. Integrar las aplicaciones y soluciones de tecnología de forma transparente a los procesos de negocio.	- % de participantes satisfechos con la integridad de los datos de los nuevos sistemas. - % de sistemas que satisfacen los beneficios esperados, tal como se midieron en el proceso posterior a la implantación.

- Garantizar el uso y desempeño apropiado de las aplicaciones y soluciones de tecnología.
- Garantizar que los servicios y la infraestructura de TI pueden resistir apropiadamente y recuperarse de fallas por errores, ataques deliberados o desastres.

PRÁCTICADE GESTIÓN RELACIONADA

AI7.2 Plan de prueba

Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito. El plan considera la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal. Con base en la evaluación de riesgos de fallas en el sistema y en la implantación, el plan deberá incluir los requerimientos de prueba de desempeño, stress, de usabilidad, piloto y de seguridad.

AI7.3 Plan de implantación

Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de versiones (Release), construcción de paquetes de versiones, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la versión y documentación de cambios. El plan deberá también incluir medidas de respaldo/ y vuelta atrás.

AI7.4 Ambiente de prueba

Establecer un ambiente de pruebas separado. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas. Se deben tener presentes los procedimientos para garantizar que los datos utilizados en el ambiente de prueba sean representativos (se limpian si es necesario). Proporcionar medidas adecuadas para prevenir la divulgación de datos sensibles. La documentación de los resultados de las pruebas se

debe archivar.
AI7.6 Prueba de cambios
Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular. Las pruebas paralelas o piloto se consideran parte del plan. Los controles de seguridad se prueban y evalúan antes de la liberación, de manera que se pueda certificar su efectividad. Los planes de respaldo/vuelta atrás se deben desarrollar y probar antes de transferir el cambio a producción.
AI7.7 Prueba final de aceptación
Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las pruebas deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba se deben salvar para propósitos de pistas de auditoría y para pruebas futuras.

Tabla .- Formulario de referencia para AI7 Instalar y acreditar soluciones y cambios (IT Governance Institute, 2007)

Fuente: Autor

3.3.4. Esquema para la recolección de información y acciones a ejecutar

La aplicación de la metodología desarrollada en la ejecución de una auditoría al área Calidad de Software de bancos medianos en Ecuador, implica utilizar los siguientes formatos para la recolección de información:

Formato para obtener la fuente de conocimiento. - En el inicio de la auditoría se hace necesario identificar las herramientas con las que se va a obtener la información. El análisis de las actividades del área que se relacionan con los objetivos de control de COBIT, generan la descripción de las acciones a ejecutar como parte de la auditoría que pueden ser: la revisión de documentación, la verificación de los flujos que se siguen en las pruebas, la aceptación de riegos durante las pruebas etc. Las herramientas pueden ser entrevistas, manuales, políticas, archivos físicos o magnéticos, reportes etc.

Este formato aplica para todos los procesos de COBIT que se van a evaluar y es responsabilidad del auditor llenar con los datos que se obtengan de las distintas fuentes de conocimiento. Si una de las fuentes de conocimiento es la entrevista, se plantea un formato genérico de entrevista que busca obtener información general de cada proceso del área.

<table>
<tr><td colspan="3">(Logo de la empresa a auditar).</td><td colspan="2">FORMATO PARA OBTENER LAS FUENTES DE CONOCIMIENTO</td><td>FECHA:
ID-FORMATO
(Identificación del formato FFC-AUD-ACC-001).</td></tr>
<tr><td colspan="2">ENTIDAD AUDITADA</td><td colspan="4">(Nombre de la entidad financiera a ser auditada).</td></tr>
<tr><td colspan="2">AREA AUDITADA</td><td colspan="4">(Nombre del área a ser auditada).</td></tr>
<tr><td colspan="2">RESPONSABLES</td><td colspan="4">(Nombre de la persona que proporciona los datos).</td></tr>
<tr><td colspan="2">AUDITORES</td><td colspan="4">(Nombre de el o los auditores).</td></tr>
<tr><td colspan="2">DOMINIO</td><td>(Nombre del dominio que se aplica para la evaluación).</td><td>PROCESO</td><td colspan="2">(Nombre del proceso que forma parte del dominio que se aplica para la evaluación).</td></tr>
<tr><td colspan="6">OBJETIVO DE CONTROL:
(Se describe el objetivo de control del proceso que se aplica para la evaluación).</td></tr>
<tr><td colspan="2">FUENTES DE CONOCIMIENTO</td><td colspan="2">DESCRIPCIÓN DEL ANALISIS DEL PROCESO</td><td colspan="2">DESCRIPCIÓN DE LAS ACCIONES A SEGUIR</td></tr>
<tr><td>1</td><td>(Espacio para identificar las herramientas que son utilizadas para obtener la</td><td colspan="2">(Espacio para la incluir el análisis de cada proceso del área, que se relaciona</td><td colspan="2">(Espacio para describir las acciones a seguir durante la ejecución de la auditoría al</td></tr>
</table>

	información).	con el objetivo de control).	proceso especifico del área auditada).

Tabla .- Formato para obtener las fuentes de conocimiento

Fuente: Autor

Formato de entrevista genérico. - Como se menciona en la sección anterior, una de las herramientas (Fuentes de conocimiento) para obtener datos relevantes son las entrevistas, que serán ejecutadas dependiendo de la necesidad de cada proceso que forma parte del flujo de certificación de una solución. Tiene como objetivo obtener información de los procesos que será analizada para generar las acciones de evaluación respectiva.

(Logo de la empresa a auditar)	**FORMATO GENÉRICO PARA ENTREVISTAS**	**FECHA:**
		ID-FORMATO
		(Identificación del formato FE-AUD-ACC-001).

ENTIDAD AUDITADA	(Nombre de la entidad financiera a ser auditada).
ÁREA AUDITADA	(Nombre del área a ser auditada).
OBJETIVO ENTREVISTA	(Determinar los procesos y actividades del área de calidad de software que serán evaluados con apoyo en los objetivos de control relacionados con cada proceso).
ENTREVISTADO	(Nombre de la persona entrevistada).
CARGO	(Cargo de la persona entrevistada).

PREGUNTAS FORMULADAS:	
1	¿Cuál es la misión y visón del área de Calidad de Software?
2	¿Cuáles son los objetivos del área de Calidad de software?
3	Cuáles son las fortalezas y debilidades presentes en el área de Calidad de Software
4	¿Cuál es la distribución de roles y responsabilidades dentro del área de Calidad de Software?
5	¿Cuáles son las herramientas tecnológicas con las que cuenta el área (Hardware y

	software)?
6	¿Dentro del ciclo de pruebas de software, cuantas y cuáles son las fases que se establecen?
7	¿Cuáles son los procesos que se ejecutan en el área de Calidad de Software?
8	¿Qué actividades se realiza en cada proceso?
9	¿Cuál es el objetivo de cada proceso?
10	¿Existen métricas para medir el cumplimiento de cada proceso, cuáles son?
11	¿De existir, cuáles son las políticas y el reglamento al que rigen las actividades del área?

Tabla .- Formato genérico de entrevistas

Fuente: Autor

3.3.5. Criterio de valoración para cada tipo de cuestionario

Se definen dos tipos de cuestionarios para la evaluación de los procesos que están inmersos en cada objetivo de control y que son ejecutados como parte del flujo de certificación de una solución en el área de calidad de software.

Cuestionarios cuantitativos que se aplicaran dependiendo del proceso y objetivo de control que se requiera evaluar. Consta de tres opciones de respuesta que pueden ser: Si, No, NA (No aplica) y el valor para cada pregunta está sujeto al criterio del auditor, de acuerdo con la importancia que le da a cada pregunta, los rangos son los siguientes:

- 1- importancia baja
- 3- importancia media
- 5- importancia alta

La sumatoria del valor de cada pregunta da el puntaje total del cuestionario. Se suman las columnas de Si, No y las NA para obtener el porcentaje de satisfacción del objetivo de control mediante el siguiente cálculo.

$$\% \text{ De satisfacción del objetivo} = \sum \text{de Si} * 100 \text{ /Totales encuesta-Totales NA}$$

Se presentan seis niveles de métrica (No existe, Inicial, Repetible, Proceso definido, Administrado y medible, Optimizado), que hacen referencia al grado de satisfacción de los objetivos de control del modelo. El grado de satisfacción se relaciona con el modelo de madurez de los procesos de COBIT de acuerdo con la siguiente tabla:

Porcentajes en intervalos	Grado de madurez de los procesos evaluados mediante los objetivos de control del modelo propuesto	Descripción
0%	No existe	No existe un proceso definido
De 1 a 20%	Inicial	El enfoque del proceso es crítico, aunque se reconoce la existencia del proceso no cumple con las necesidades expuestas en los objetivos de control del modelo
De 20 a 40%	Repetible	Se alinea medianamente a los objetivos del modelo, cumpliendo parcialmente las necesidades de control
De 40 a 60%	Proceso definido	Ya se cuenta con un proceso definido y alineado con los objetivos de control. Genera dudas, pero son solventadas
De 60 a 80%	Administrado y medible	Los objetivos del modelo se cumplen organizadamente, mediante la ejecución de procesos formales y estructurados

De 80 a 100%	Optimizado	El proceso presenta un alto nivel de adhesión a los objetivos del modelo.

Tabla .- Tabla de valores para la evaluación de cada proceso de forma cuantitativa

Fuente: Autor

Cuestionarios cualitativos, al igual que el cuestionario anterior aplica dependiendo el objetivo de control a evaluar. Se realizan preguntas relacionadas con el desempeño del proceso, siendo los posibles parámetros los siguientes: siempre, casi siempre, usualmente, a veces, rara vez y nunca.

Cada posible respuesta tiene una única interpretación y un valor que luego de realizar el cálculo respectivo se ubica cada proceso en un rango porcentual. Este rango indica el nivel de desempeño y cumplimiento en relación con el objetivo de control del modelo propuesto. El valor para cada parámetro se distribuye de la siguiente manera:

Parámetro	Valor
Nunca	0
Rara vez	1
A veces	2
Usualmente	3
Casi Siempre	4
Siempre	5

Tabla .- Parámetros para el cuestionario cualitativo

Fuente: Autor

Bajo la misma premisa de la ponderación anterior, se suman los valores de todos los parámetros que se registran para cada pregunta y se multiplican por el 100%, que corresponde al total de respuestas y se divide para la suma total del mayor valor posible. Con esto se obtiene el porcentaje de cumplimiento del objetivo de control.

$$\%\ De\ cumplimiento\ del\ objetivo = \sum de\ Todos\ los\ valores * 100\ /Total\ Mayor\ valor\ posible$$

Porcentajes en intervalos	Nivel de desempeño que se relaciona con el grado de madurez de los procesos	Descripción
0%	No existe	
De 1 a 20%	Inicial	Es un proceso que existe, pero ejecuta medias lo requerido en el objetivo de control. Las metas específicas no están acordes con lo que se necesita en el área y menos para la organización.
De 20 a 40%	Repetible	Un proceso repetible satisface metas específicas y se alinea con las metas de TI (Calidad de Software); sigue lo requerido por el objetivo de control. Aunque se tiene mejoras importantes, estas pueden perderse en el tiempo si no se las sigue poniendo en práctica
De 40 a 60%	Proceso definido	El proceso se ejecuta a la medida de lo requerido por su objetivo de control. Está fundamentado en procesos y estándares que satisfacen ciertas necesidades del flujo general
De 60 a 80%	Administrado y medible	El proceso o actividad se ejecuta acorde con lo requerido en el objetivo de control, con un porcentaje alto de cumplimiento
De 80 a 100%	Optimizado	La actividad o el proceso se alinean, llegando a cumplir un 100% del

	tiempo con lo requerido por el objetivo de control

Tabla .- Tabla de valores para la evaluación de cada proceso de forma cualitativa

Fuente: Autor

3.3.5. Implementación de cuestionarios de evaluación basados en el modelo

AUD-ACC-PO4.7-001	Verificar la existencia de un organigrama donde se definan de forma clara funciones, roles y responsabilidades de los integrantes del área. Se comprueba si se está evaluando periódicamente que el personal tenga las habilidades para cumplir sus roles y que estén relacionadas con su educación, capacitación y experiencia.				
Dominio	Planear y organizar.				
Proceso	Definir los procesos, organización y relaciones de TI.				
Control	Responsabilidad de aseguramiento de calidad de TI.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	Existe un organigrama de la organización, donde se muestre la estructura funcional del área.				
2	Están descritas en un manual de funciones y competencias, las funciones y responsabilidades para cada rol dentro del área.				
3	Se encuentran debidamente documentadas las políticas de control y seguimiento a las actividades del área.				
4	Se tienen identificadas las responsabilidades que requieren mayor atención, dentro de la segregación de funciones.				
5	Existen perfiles dentro del área que no están cubiertos.				
6	El perfil de cada colaborador está relacionado con				

	lo requerido para cada función.				
7	Se asignan funciones de acuerdo con el perfil de cada colaborador.				
8	Se asignan de forma balanceada las tareas para cada recurso del área.				
9	Los tiempos de duración de cada tarea se relacionan con su complejidad.				
10	Existe un plan de carrera profesional que se ejecuta con base a la experiencia, conocimientos y capacitaciones realizadas.				
Observaciones:					

Criterio de evaluación		**Nunca**	**Rara vez**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**
1	Se realizan evaluaciones para determinar las habilidades de cada colaborador.						
2	Se realizan capacitaciones para actualizar los conocimientos del personal.						
3	Se realizan reuniones entre los colaboradores y la dirección del área.						
4	Se incentiva de alguna manera a los colaboradores del área, por objetivos cumplidos.						
5	Se da las facilidades al						

	personal para el crecimiento profesional y académico.						
6	El personal trabaja fuera de horario.						
7	La dirección del área se muestra satisfecha con las tareas ejecutadas en el área.						
8	Las tareas son distribuidas al personal del área, de acuerdo con la carga laboral de cada recurso.						
9	La revisión de prioridades de cada tarea es realizada.						
10	La rotación de personal en el área se presenta.						
Observaciones:							

Tabla .- Cuestionario para PO4.7 Responsabilidad de aseguramiento de calidad de TI

Fuente: Autor

AUD-ACC-PO8.1-002	Medir la calidad del servicio que brinda el área de control de calidad de software.				
Dominio	Planear y organizar.				
Proceso	Administrar la calidad.				
Control	Sistema de administración de calidad.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	La dirección ha desarrollado, implementado y mejorado sus capacidades de administración de la				

	calidad en el área.				
2	Existe una caracterización de los procesos que se ejecutan dentro del Área de Calidad de Software.				
3	Se realiza una planificación adecuada, para la administración de la calidad del servicio, que asegure la calidad de los sistemas.				
4	Existen objetivos planteados en el área, para realizar una administración adecuada del servicio.				
5	Existen mecanismos que implemente mejora continua.				
6	Se han definido acuerdos de niveles de servicio con las otras áreas.				
7	El área cuenta con recursos humanos suficientes para cubrir la demanda.				
8	Existe una buena relación con las áreas que se interactúa frecuentemente.				
9	Se conoce y se realiza una buena gestión de las necesidades del área.				
10	Se realizan un análisis para determinar las causas de los problemas del área.				
Observaciones:					

Criterio de evaluación		**Nunca**	**Rara vez**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**
1	El cumplimiento de los objetivos planteados por el área se evalúa.						
2	La socialización de los objetivos del área se realiza.						
3	El área tiene la capacidad de cubrir la demanda.						

4	La supervisión y seguimiento de las actividades que se ejecutan en el área se realiza.						
5	En el área se cumplen los tiempos de acuerdo con lo planificado.						
6	Se han ejecutado reversos en producción por errores no detectados en el proceso de certificación.						
7	En el área se identifican problemas de forma proactiva.						
8	Se gestionan los suministros necesarios para el área.						
9	Existen cambios en el servicio que afectan el desempeño.						
10	Se realiza la revisión de la calidad del servicio en el área.						
Observaciones:							

Tabla .-Cuestionario para PO8.1 Sistema de administración de calidad

Fuente: Autor

AUD-ACC-PO8.2-003	Verificar la existencia de estándares y procedimientos que orienten a la organización y específicamente al área de calidad de software, al cumplimiento de lo planteado como objetivos en la administración de la calidad del servicio.
Dominio	Planear y organizar.

Proceso	Administrar la calidad.				
Control	Estándares y prácticas de calidad.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	La administración de la calidad del servicio se ejecuta con base en normas, estándares y metodologías.				
2	Se ha realizado un estudio sobre que estándares, procedimientos y metodologías, son los más adecuados para aplicarlos en los procesos que se ejecutan en el área.				
3	Las políticas, normas, estándares, metodologías y prácticas de calidad satisfacen los objetivos de la administración del servicio.				
4	Se han definido políticas, estándares y procedimientos que controlen las actividades que se ejecutan en el área.				
5	Los estándares relacionados con prácticas de aseguramiento de la calidad se alinean con los procesos del área.				
6	Los estándares y prácticas de calidad que se utilizan para lograr una administración de la calidad del servicio son aprobados por la dirección				
7	La metodología, estándares y prácticas de calidad son difundidas en el entorno del área.				
8	Se ha evaluado el desempeño de los estándares, metodologías y prácticas de calidad.				
9	Se ha identificado en el área el incumplimiento de normas y estándares establecido para administrar el servicio de calidad.				
10	Existe información suficiente acerca de los				

	estándares que se utilizan en el área.				
Observaciones:					

Tabla .- Cuestionario para PO8.2 Estándares y prácticas de calidad

Fuente: Autor

AUD-ACC-PO8.1-004	Medir el cumplimiento de los objetivos planteados como parte de la administración de calidad del servicio. La medición registra información en general de los procesos del área.				
Dominio	Planear y organizar.				
Proceso	Administrar la calidad.				
Control	Medición, monitoreo y revisión de la calidad.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	Existe documentación de los procesos que se ejecutan como servicio de calidad de software.				
2	Existe satisfacción en los clientes internos con el servicio que se está brindado por parte del área.				
3	El área se encuentra mejor situada en cuanto a la calidad del servicio en relación con las demás.				
4	Existe satisfacción interna en el área con el servicio que se está brindando.				
5	Se asegura de alguna manera que el servicio satisfaga y aporte al desenvolvimiento de las demás áreas.				
6	El servicio impacta en los objetivos de calidad de la organización.				
7	Existen indicadores para medir los procesos del área.				
8	Se toman en cuenta sugerencias y recomendaciones de otras áreas para mejorar el servicio que brinda el área.				
9	Los documentos que se utilizan como parte de los procesos que se siguen en el área son entendibles.				
10	Se presentan informes de gestión por parte de la dirección del área.				
Observaciones:					

Tabla .- Cuestionario para PO8.6 Medición, monitoreo y revisión de la calidad

Fuente: Autor

AUD-ACC-AI2.8-005	Se encamina a verificar que los proyectos cuenten con un plan de aseguramiento de calidad del software donde se definan los requerimientos, estándares y procedimientos de calidad que busca una organización.				
Dominio	Adquirir e implementar.				
Proceso	Adquirir y dar mantenimiento a software aplicativo.				
Control	Aseguramiento de la calidad del software.				
Auditor					
Responsable		**Fecha:**			

Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	Se genera un plan de aseguramiento de la calidad como parte del servicio que proporciona el área.				
2	El plan de aseguramiento de la calidad se encuentra debidamente documentado.				
3	El plan de aseguramiento de la calidad es revisado y aprobado por los interesados.				
4	Las actividades que se siguen como parte de la certificación de un producto de software, están dentro del plan de aseguramiento de la calidad.				
5	Las inconformidades encontradas durante el proceso de certificación de un producto de software siguen un procedimiento establecido para su solución.				
6	Se ha modificado el plan de aseguramiento de la calidad establecido en un inicio por las necesidades de un proyecto o requerimiento.				
7	El equipo de calidad informa regularmente de las novedades presentadas en el proceso, a los equipos relacionados.				
8	En el área se cuenta con herramientas para la administración de las novedades e inconformidades				

	presentadas.					
9	De acuerdo con lo establecido como requerimientos de calidad, se cumple con los tiempos estimados de entrega de las certificaciones.					
10	Se cuenta con indicadores que muestran los errores presentados en el ambiente de pruebas.					
Observaciones:						

Criterio de evaluación		**Nunca**	**Rara vez**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**
1	Los integrantes del equipo de calidad se capacitan para realizar el plan de aseguramiento de calidad.						
2	El equipo de calidad participa en la definición de requerimientos.						
3	El seguimiento realizado a las inconformidades presentadas es:						
4	Se priorizan los requerimientos con base en la relevancia del negocio.						
5	Se identifica cada incumplimiento encontrado durante la certificación de un						

	producto de software.						
6	En el área se documentan las lecciones aprendidas durante el proceso.						
7	Son usados los criterios de calidad durante el proceso de certificación de un producto de software.						
8	Se comunica la presencia de inconformidades y se asegura su resolución.						
9	Se realiza informes de avance de las pruebas con las respectivas novedades presentadas.						
10	Se revisa el historial de pruebas de un producto de software antes de dar la certificación.						
Observaciones:							

Tabla .- Cuestionario AI2.8 Aseguramiento de la calidad del software

Fuente: Autor

AUD-ACC-AI7.2-006	Validar cada una de la interacción que se generan de la existencia de un plan de prueba, que incluye los pasos a seguir durante el proceso de certificación de un producto de software y la forma de identificar las novedades presentadas.				
Dominio	Adquirir e implementar.				
Proceso	Instalar y acreditar soluciones y cambios.				
Control	Plan de prueba.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	Se genera un plan de pruebas que especifique las actividades a ejecutar durante el ciclo de pruebas.				
2	El plan de pruebas es documentado, revisado y aprobado por la dirección del área.				
3	Como parte del plan de pruebas se definen además de las pruebas funcionales, pruebas como seguridad y rendimiento.				
4	Se define claramente el alcance de las pruebas.				
5	La obtención de data es una tarea que se encuentra en el plan de pruebas.				
6	Se han definido criterios de aceptación tanto para pruebas funcionales y no funcionales.				
7	Se tiene planteado dentro del plan de pruebas, una estrategia de ejecución de pruebas que contemple todos los posibles escenarios.				
8	Como parte de las tareas se encuentra la elaboración de casos de prueba.				
9	Se presenta una estimación de tiempos que se relaciona con un cronograma para el ciclo de pruebas.				
10	Existe una metodología para llevar a cabo el plan de pruebas.				
Observaciones:					

Criterio de evaluación	**Nunca**	**Rara**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**

			vez			**e**	
1	Se establece un plan de pruebas detallando el alcance de las pruebas y las tareas a ejecutar.						
2	Se realiza una estimación de la duración de las tareas, mediante algún diagrama o método.						
3	Se define el ciclo de pruebas.						
4	Se identifican riesgos inherentes al requerimiento o al desarrollo de software a certificar.						
5	Se establece en el plan equipos, software asociado o recursos humanos que se necesitaran para la ejecución de las pruebas.						
6	Se incluye en el plan la información de los requisitos que se deben cumplir antes de empezar con las pruebas.						
7	Se definen los tipos						

	de prueba a ejecutar.						
8	Se elaboran los casos de prueba en relación con los requerimientos funcionales y no funcionales.						
9	Se plantea en el plan la validación del entorno, previo a la ejecución de pruebas.						
10	Se recibe la aceptación del plan de pruebas por parte de los involucrados.						
Observaciones:							

Tabla .- Cuestionario para AI7.2 Plan de prueba

Fuente: Autor

AUD-ACC-AI7.4-007	Se busca mediante este cuestionario verificar varios aspectos para tener en cuenta en un ambiente de pruebas: - Mantener ambientes separados para desarrollo, pruebas y producción. - El ambiente debe ser en lo posible similar al de producción para permitir pruebas más acertadas. - Los datos deben ser representativos en una proporción considerable en relaciona la data que existe en producción. - Proporcionar medidas adecuadas para prevenir la divulgación de datos sensibles. - Documentación de los de los ambientes (información de hardware y software).
Dominio	Adquirir e implementar.

Proceso	Instalar y acreditar soluciones y cambios.		
Control	Ambiente de prueba.		
Auditor			
Responsable		**Fecha:**	

	Criterio de evaluación	**Importancia**	**Si**	**No**	**NA**
1	El ambiente de pruebas reside en un servidor compartido por los equipos de pruebas.				
2	El ambiente de prueba es similar al de producción				
3	La información de los ambientes de prueba está documentada y es accesible al equipo de pruebas.				
4	El ambiente de pruebas es administrado por personal que no hace parte del equipo de pruebas.				
5	Se realizan controles de cambio que mantengan el rastro de las modificaciones realizadas en la configuración del ambiente.				
6	Las versiones que van a ser instaladas en producción fueron probadas previamente en el ambiente de pruebas.				
7	Se realiza comprobaciones frecuentes de la configuración de ambientes.,				
8	Se homologan al ambiente de pruebas los cambios de emergencia realizados en producción.				
9	Se tiene procedimientos para solicitud de un ambiente de pruebas.				
10	Los datos del ambiente de pruebas están ofuscados.				
Observaciones:					

	Criterio de evaluación	**Nunca**	**Rara vez**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**
1	Se planifican actividades de mantenimiento del						

	ambiente de pruebas.						
2	Se realizan verificaciones del ambiente, antes de iniciar un ciclo de pruebas.						
3	Se cuenta con herramientas de control de versiones, para no afectar el ambiente cuando existen múltiples requerimientos en vuelo.						
4	Se realizan pruebas directamente en la ambiente producción.						
5	En los reportes de incidentes, se detalla el ambiente en el que se está probando.						
6	Se han realizado pruebas en un ambiente de desarrollo.						
7	Los ambientes de pruebas son estables.						
8	Se mantiene un						

	registro de la inestabilidad del ambiente pruebas.						
9	Se realizan cambios de configuración en el ambiente, durante la ejecución de las pruebas.						
10	Se generan simuladores que son parte del entorno de pruebas.						
Observaciones:							

Tabla .- Cuestionario para AI7.4 Ambiente de prueba

Fuente: Autor

AUD-ACC-AI7.4-007	A través de este cuestionario se pretende conocer si los cambios que se relacionan con errores preexistentes o generados por fallas del software y cuya solución requieren se ejecuten de manera inmediata, siguen un proceso que en efecto sea una solución y no se convierta en un parche que puede generar más errores a futuro.				
Dominio	Adquirir e implementar.				
Proceso	Instalar y acreditar soluciones y cambios.				
Control	Prueba de cambios.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**
1	Existe un plan para el manejo de incidentes de rápida solución.				
2	Se mantiene la trazabilidad de cada incidente.				
3	Se tiene un proceso de atención de incidentes				

	generados en producción.				
4	Los incidentes se catalogan de acuerdo con su criticidad e impacto.				
5	Se tiene un registro de incidentes que analice cual fue la causa y efecto.				
6	Se tiene un archivo de información sobre la solución y el trato que se le ha dado a cada incidente				
7	Se han hecho pruebas directamente en producción para la solución de un incidente.				
8	Se realiza un monitoreo en producción para identificar los errores preexistentes.				
9	Se conoce si se han generado otros incidentes, luego de la implementar la solución de un incidente en producción.				
10	Se tiene un tiempo de atención de cada incidente dependiendo su criticidad.				
Observaciones:					

Tabla .- Cuestionario para AI7.6 Prueba de cambios

Fuente: Autor

AUD-ACC-AI7.4-007	Mediante la ejecución de este cuestionario se busca determinar, si los cambios son probados de acuerdo con lo requerido. Además, se debe seguir lo expuesto en el plan de pruebas, donde se consideran los diferentes escenarios de prueba.				
Dominio	Adquirir e implementar.				
Proceso	Instalar y acreditar soluciones y cambios.				
Control	Prueba final de aceptación.				
Auditor					
Responsable		**Fecha:**			
Criterio de evaluación		**Importancia**	**Si**	**No**	**NA**

1	Se ejecutan todos los ciclos de prueba de acuerdo con lo planificado.				
2	Se tiene un proceso para el manejo de inconsistencias e incidentes durante la ejecución de pruebas.				
3	El set de datos con el que se ejecuta las pruebas se ajusta a la necesidad de cada requerimiento.				
4	Los casos de prueba son claros al momento de ejecutarlos.				
5	Se ejecutan casos automatizados.				
6	Se genera informes diarios de avance de la ejecución de pruebas.				
7	Se documentan las evidencias de la ejecución de pruebas en herramientas adecuadas.				
8	Se mantiene un archivo de lecciones aprendidas de los errores de ejecución que se cometen.				
9	Las pruebas de rendimiento y seguridad las realiza la misma persona que ejecuta las pruebas funcionales				
10	Existe un documento de riesgos asumidos para los casos que no se prueban por diferentes motivos.				
Observaciones:					

Criterio de evaluación		**Nunca**	**Rara vez**	**A veces**	**Usualmente**	**Casi Siempre**	**Siempre**
1	Se devuelve un proyecto o requerimiento si no cumple con lo requerido para el inicio de las pruebas formales.						

2	Se cumplen los tiempos de ejecución de pruebas de acuerdo con lo previsto.						
3	Se ejecutan el total de casos de prueba.						
4	Los criterios de aceptación son definidos por personal especializado.						
5	Se cumple con los criterios de aceptación para la certificación de un nuevo software o su actualización.						
6	Las pruebas sobre simuladores son confiables.						
7	Se realiza un seguimiento de los errores encontrados en la etapa de ejecución de pruebas.						
8	Los escenarios de pruebas son lo más reales posible.						
9	Se corrigen con rapidez errores bloqueantes.						
10	Se realiza una revisión por parte del líder del encargado de supervisar las pruebas,						

	del informe final antes de emitir su certificación.						
Observaciones:							

Tabla .- Cuestionario para AI7.7 Prueba final de aceptación

Fuente: Autor

3.4. Fases de la Metodología propuesta

Para realizar una auditoría y específicamente al área de Calidad de Software de entidades financieras medianas en Ecuador, se requiere seguir una serie ordenada de pasos que ejecutan acciones y procedimientos que son diseñados previamente. Esto con el fin de cumplir con todas las etapas establecidas con base en las necesidades de cada organización.

Esta metodología considera un estudio preliminar y tres fases durante el proceso (Planeación, Ejecución, Informe) que contienen aspectos específicos para cada fase transformados en pasos.

3.4.1. Antecedentes de la auditoría

Se considera importante antes de iniciar con las fases de la auditoría, tener claros algunos aspectos que servirán de base para su desarrollo efectivo. Entre los temas a considerar están:

Origen de la Auditoría. - Es el punto inicial de la auditoría y busca determinar quién es el responsable o de acuerdo con que necesidades se realiza la solicitud para la ejecución de una auditoría.

Alcance de la auditoría. - Se enfoca en delimitar el área donde se va a efectuar la auditoría, permite identificar qué objetivos de control serán parte de la revisión. Como parte del alcance de la auditoría, se establecen factores que permiten verificar la satisfacción y el cumplimiento de los objetivos de control.

Objetivos de la auditoría. - Se relacionan con las causas por las que se solicita la auditoría.

Puntos para evaluar. - Aquí se debe especificar de forma puntual cuáles serán los puntos clave a evaluar, siendo en este caso los procesos genéricos que pueden estar presentes directa e indirectamente en el área de Calidad de Software en una entidad financiera u organización y que se contemplan dentro de la metodología propuesta.

Documentos para solicitar. - Para la evaluación de cada proceso mediante los objetivos de control de COBIT utilizando las herramientas de recolección de datos, se debe solicitar los documentos que respalden la afirmación de varias de las inquietudes planteadas en los cuestionarios y entrevistas que se plantean en la sección Implementación de cuestionarios de evaluación basados en el modelo. Estos pueden ser entre otros los que se enumeran en la tabla siguiente y se deben estar registrados de acuerdo con el siguiente *checklist* de verificación:

Nombre de la entidad auditada **Nombre del área Auditada**	**PERIODO DE REVISIÓN**
PARA: **Nombre y cargo de la persona responsable del área**	**DE:** **Nombre de auditor líder** **Auditor de TI**
Asunto: Solicitud de Información para Auditoría del área de Calidad de Software Reciba un cordial saludo del equipo de Auditoría TI, por medio de la presente solicitamos su gentil ayuda para que se facilite la información que se describe en los ítems siguientes:	

Documentos:	**Existen**		**Observaciones:**
	Si	**No**	
Políticas			
Estándares			
Estatutos, reglamentos internos			
Manual de procesos			
Manual de calidad			
Plan de pruebas			
Informe de pruebas			

Lecciones aprendidas			
Bitácora de incidentes			
Documentos funcionales			
Diagrama de los procesos			
Reportes, etc.			
La información existente se debe entregar al equipo de auditoría, hasta el (fecha límite de entrega de documentos según el cronograma) del presente año y debe ser remitida en formato digital o físico. Seguros de contar con su colaboración, agradecimiento de antemano. Atentamente; ---------- Nombre del auditor líder			

Tabla .Listado de verificación y solicitud de documentos

Fuente: Autor

De haber más tipos de documentos de respaldo, se los debe agregar y verificar su existencia en el mismo *checklist*.

Grupo de trabajo. - Son los participantes de la auditoría que se distribuyen entre el equipo auditor y de ser necesario personal propio del área u organización a auditar. Todo el proceso de auditoría debe estar liderado por un auditor líder del equipo.

3.4.2. Fase de planeación de la auditoría

Paso 1.- Estudio preliminar

De manera práctica el auditor deberá buscar información a través de las personas responsables en el área de Calidad de Software, con la ayuda de herramientas que facilitan la recolección de información que en este caso es una entrevista genérica con preguntas puntuales que ayudaran a presentar información como:

- **Estructura organizacional del área de Control de Calidad de Software. -** Aquí se debe obtener información como la visión, misión, organigrama del área, fortalezas y debilidades del área, objetivos del área, diagrama de los procesos del área.
- **Distribución de funciones en el área de Control de Calidad de Software**. - Se consigue como resultado la segregación de funciones, con la descripción de roles y responsabilidades.
- **Recursos tecnológicos con los que cuenta el área de Calidad de Software. -** Hace referencia a toda la ayuda tecnología sea hardware o software que se utiliza para el proceso de certificación de un requerimiento de software.

Paso 2.- Estrategia de auditoría al área de Calidad de Software

La estrategia de una auditoría en general representa el soporte para las actividades que se realizan durante la ejecución de la auditoría. La metodología propuesta incluye en su modelo la estrategia a seguir con base en el marco de referencia COBIT, que se estructura de la siguiente manera:

- **Justificación de la metodología utilizada**. - Se entiende que al ser la metodología propuesta una opción entre otras, se debe justificar su utilización tomando en consideración que está basada en el marco de referencia COBIT.
- **Determinación del modelo de evaluación según la metodología**. - Al ser una metodología basada en COBIT, se genera un modelo que está orientado a evaluar los procesos del área de Calidad de Software, mediante Objetivos de Control que se relacionan con Procesos que se derivan de Dominios de control. En la metodología propuesta se tiene cuatro procesos con nueve objetivos de control que evalúan las actividades y procesos que se ejecutan como parte del proceso de certificación de un requerimiento que genera de un producto de software. Se enfocan en los siguientes elementos:

  1. **El área donde se ejecuta la auditoría. -** El área como parte de la organización controla y administra los recursos humanos y tecnológicos mediante procesos que deben ser evaluados para determinar su eficacia con lo requerido por el negocio.
  2. **Procesos del modelo metodológico. -** La evaluación de los procesos y actividades del área de Calidad de Software, basa su relación en 4 procesos de

los 34 procesos definidos por COBIT, como se estructuró en la sección donde se define el Modelo de evaluación que establece la metodología.

3. **Objetivos de Control. -** Según el modelo de la metodología propuesta se tiene nueve Objetivos de Control que se deben cumplir y satisfacer por cada uno de los procesos evaluados.

4. Mediciones e indicadores. - Cada proceso se evalúa mediante herramientas para la obtención de información, como cuestionarios que una vez ponderados generan dos indicadores: el porcentaje de satisfacción de los objetivos de control y el cumplimiento de estos.

Estos a su vez se mapean con el nivel de madurez que COBIT implementa para medir cada proceso, tal y como se encuentra detallado en el Esquema para la recolección de información.

- **Definición del programa de auditoría. -** Se constituye en una guía metodológica para la ejecución del proceso de auditoría, que analiza y evalúa de acuerdo con los parámetros que se contemplan en la estrategia y que son parte del modelo. La aplicación de este programa permite conocer el grado de cumplimiento, satisfacción y estado en el que se encuentran los procesos que son empleados en el área.

Se plantea el programa de acuerdo con las etapas que se cumplen durante el proceso de certificación como se muestra a continuación:

Tabla .- Programa de auditoría
Fuente: Autor

PROGRAMA DE AUDITORÍA															
Objetivos de control:	**Criterios de la Información**							**Procesos Genéricos**	**Técnicas por ejecutar**	**Recursos de TI**				**Instrumento Utilizado**	**Documento de Referencia**
	1	**2**	**3**	**4**	**5**	**6**	**7**			**A**	**B**	**C**	**D**		
PO4.7 Responsabilidad de aseguramiento de calidad de TI	**P**	**P**						Organigrama del área, roles y responsabilidades de sus integrantes	- Realizar una entrevista genérica al personal encargado del área.				**X**	Entrevista	Tabla 15 Formato genérico de entrevistas
									Realizar los siguientes cuestionarios: - Cualitativos y - Cuantitativo Nota: El valor asignado depende del Auditor					Cuestionario	Cuestionario para PO4.7 Responsabilidad de aseguramiento de calidad de TI
PO8.1 Sistema de administración de calidad	**P**	**P**		**S**			**S**	Establecer y mantener un sistema para la Administración de la calidad, el seguimiento continuo de la ejecución de las pruebas e implementar programas para la mejora continua	Realizar los siguientes cuestionarios: - Cualitativos y - Cuantitativo Nota: El valor asignado depende del Auditor	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para PO8.1 Sistema de administración de calidad
PO8.2 Estándares y prácticas de calidad	**P**	**P**		**S**			**S**	Se incluya en la ejecución de los procesos del área metodologías, mejores prácticas, estándares, procedimientos y políticas claras de calidad	Realizar el cuestionario que permite verificar la interacción en el área con estándares, procedimientos y políticas claras de calidad.	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para PO8.2 Estándares y prácticas de calidad
PO8.6 Medición, monitoreo y revisión de la calidad	**P**	**P**		**S**			**S**	El monitoreo y revisión interno y externo constante del desempeño y mejora continua del cumplimiento de los procesos, se reflejará en un registro de la información que se usará para aplicar medidas correctivas	Realizar el cuestionario que permite validar los procesos de la mejora continua	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para PO8.6 Medición, monitoreo y revisión de la calidad
AI2.8 Aseguramiento de la calidad del software	**P**	**P**		**S**			**S**	Se cubre las expectativas del negocio a través de requerimientos que son cubiertos en su totalidad en el menor tiempo, con un bajo costo y sin reproceso por problemas que se puedan generar en producción	Dos cuestionarios que se encargan de verificar que los requerimientos y proyectos que solicitan el servicio que brinda el área, cumplan con lo planteado en el plan de aseguramiento de la calidad.			**X**		Cuestionario	Cuestionario AI2.8 Aseguramiento de la calidad del software

AI7.2 Plan de prueba	**P**	**S**		**S**	**S**			Proceso que establece un plan de pruebas que contempla todas las etapas del proceso de certificación y que se ajuste a la metodología de pruebas utilizada. El proceso de definición de roles y responsabilidades es aplicado para la asignación de las tareas al personal del área.	Dos cuestionarios que evalúan lo mínimo que debe incluir el plan de pruebas para que signifique un aporte importante en el proceso de pruebas de un requerimiento o proyecto que genere un producto de software.	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para AI7.2 Plan de prueba
AI7.4 Ambiente de prueba	**P**	**S**		**S**	**S**			Mantener un ambiente para pruebas dedicado, con datos de prueba relevantes y que se asemeje en su infraestructura (hardware, software y arquitectura) con el ambiente de producción	Realizar dos cuestionarios para validar cuantos ambientes de pruebas tiene la empresa	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para AI7.4 Ambiente de prueba
AI7.6 Prueba de cambios	**P**	**S**		**S**	**S**			Los cambios que se generan por fallas o incidentes encontrados en producción están sujetos a un plan preestablecido para el manejo de incidentes garantizando que la trazabilidad no se vea afectada y se pueda conocer el origen, causas y la solución al incidente lo que implica mantener un archivo de lecciones aprendidas. Las actividades ejecutadas deben respaldarse con pistas de auditoría.	Realizar un cuestionario que permita validar y registrar los incidentes que se presentan en el Área de Calidad	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para AI7.6 Prueba de cambios
AI7.7 Prueba final de aceptación	**P**	**S**		**S**	**S**			Garantizar que exista una evaluación formal que cubra todos los posibles escenarios de prueba, así como la interacción con los componentes del sistema (hardware, software, y procedimientos de tecnología). Los resultados que se obtengan deben ser revisados y aprobados por un responsable previamente designado, además se debe documentar adecuadamente para revisiones futuras	Realizar dos cuestionarios que permitan validar las Pruebas, ensayos y pilotos del servicio Validación y prueba del servicio y la ejecución de las pruebas y evaluar los criterios y reportes de salida; la finalización y cierres	**X**	**X**	**X**	**X**	Cuestionario	Cuestionario para AI7.7 Prueba final de aceptación

Equivalencias:

Recursos de TI	
A	Aplicaciones
B	Información
C	Infraestructura
D	Personas

Criterios de la Información		
1		Efectividad
2		Eficiencia
3		Confidencialidad
4		Integridad
5		Disponibilidad
6		Cumplimiento
7		Confiabilidad

Cada una de las herramientas o técnicas utilizadas ya sea para realizar una entrevista o para obtener los datos relevantes a través de cuestionarios, se detallan en la sección de Implementación de cuestionarios propuestos en el modelo de la metodología.

- **Cronograma de la auditoría. -** Es fundamental mantener el control del avance de la auditorÍa, por lo que la elaboración de un cronograma es una herramienta útil que ayuda a cumplir con este objetivo.

Paso 3.- Formato para la generación del plan de auditoría. - Se define un formato que se genera como un resumen del plan de auditoría el mismo que se presenta de la siguiente manera:

Sello de la organización donde se realiza la auditoría	**PLAN DE AUDITORÍA**	**Código del documento**	**FECHA:**
		Versión 1.0	
OBJETIVO:			
ALCANCE:			
CRITERIO METODOLOGICO: (mencionar el modelo metodológico utilizado)			
TECNICAS Y PROCEDIMIENTOS: (fuentes de conocimiento utilizadas entrevistas, cuestionarios etc.)			
EQUIPO AUDITOR: (Auditor líder, experto técnico, auditores juniores, etc.)			
RESPONSABLE DEL AREA:			
Reunión de apertura: (fecha de inicio de la auditoría)	**Sitio:** (dirección donde se realiza la auditoría)		
EXCLUSIONES:			

ACTIVIDADES DE LA AUDITORÍA	AUDITADOS CARGO Y NOMBRE	AUDITOR	FECHA	HORA	SITIO
Reunión de socialización de la auditoría					
Realizar Entrevista a él o los líderes del área					
Solicitud de Información y Documentación					
Verificar Perfiles, Roles y Responsabilidades					
Evaluar los procesos del área de Control de Calidad de software					
Interpretación de resultados de la evaluación					
OBSERVACIONES:					

Tabla .- Formato del plan de auditoría

Fuente: Autor

3.4.3. Fase de ejecución de la auditoría

Es la fase donde se ejecutan las actividades que pretenden evaluar los procesos del área de Calidad de Calidad de Software, que se relacionan con los procesos y sus objetivos de control de acuerdo con el marco de referencia COBIT, para así determinar su nivel de madurez.

3.4.3.1. Procesos y actividades para ejecutar durante la auditoría

El proceso de auditoría que se diseña deberá relacionar las actividades a realizar con la necesidad de obtener información relevante que se analizará en todo el proceso. Estas actividades serían las siguientes:

- **Reunión de socialización de la auditoría. -** Es solicitada directamente por el auditor líder y tiene como objetivo dar a conocer el equipo de auditoría o la persona que puede ser el líder y auditor que ejecuta las acciones durante el proceso. Además,

se socializa sobre los principales puntos y características que tendrá la auditoría a ejecutarse en el área y se dará inicio a la misma.

- **Realizar entrevista a los líderes del área. -** Para realizar esta actividad se tiene previsto ejecutar el cuestionario para la obtención de fuentes de conocimiento y el cuestionario genérico de entrevista que se encuentran en la sección Esquema para la recolección de información. El objetivo es obtener información general pero muy útil que servirá de base para la ejecución de las demás actividades.

- **Solicitud de Información y Documentación. -** Durante la ejecución de cada actividad, se ejecutarán cuestionarios que validarán información que justifique una respuesta positiva, mediante la solicitud de documentos o información que respalde la afirmación realizada.

- **Verificar Perfiles, Roles y Responsabilidades. -** Corresponde a la validación mediante el primer objetivo de control que corresponde a la segregación de funciones y aunque no es parte de los procesos del área de Calidad de Software, influye en el correcto desarrollo de los demás procesos que si son parte. Se evalúa mediante la ejecución de la entrevista genérica y dos cuestionarios como se especifica en la sección que corresponde al Esquema de recolección de información.

- **Evaluar los procesos del área de Calidad de Software. -** Al igual que en el paso anterior se pretende mediante la ejecución de cuestionarios, evaluar el grado de cumplimiento y satisfacción que generan los procesos del área en relación con los objetivos de control mapeados tal y como se muestra en la sección Selección de los dominios y procesos de COBIT.

- **Interpretación de resultados de la evaluación. -** En este punto se realiza la ponderación de los resultados que se generan y que luego serán plasmados en el informe final que evalúan el cumplimiento y satisfacción de los objetivos de control.

3.4.4. Fase de entrega del informe de la auditoría

Corresponde a la última fase de la auditoría donde se presenta un resumen de los resultados de la evaluación, de acuerdo con la relación de los procesos de COBIT y sus objetivos de control con los procesos del área. Este informe se presenta en un documento que se denomina, "Informe final de los resultados de la Auditoría". Sin embargo, se debe detallar en los anexos los resultados de la evaluación para cada uno del proceso.

3.4.4.1. Elaboración del documento "Informe final de los resultados de la Auditoría"

Siendo el informe un documento que resume los resultados de la auditoría, es necesario tener una estructura que se la presenta de la siguiente manera:

<table>
<tr><td rowspan="2">Sello de la organización donde se realiza la auditoría</td><td colspan="2" rowspan="2">INFORME DE AUDITORÍA</td><td>Código del documento</td><td>FECHA:</td></tr>
<tr><td>Versión 1.0</td><td></td></tr>
<tr><td colspan="2">NOMBRE DE LA ENTIDAD:</td><td colspan="3"></td></tr>
<tr><td colspan="2">OBJETIVO GENERAL:</td><td colspan="3"></td></tr>
<tr><td colspan="2">OBJETIVOS ESPECIFICOS:</td><td colspan="3"></td></tr>
<tr><td colspan="2">LUGAR DE LA AUDITORÍA:</td><td colspan="3"></td></tr>
<tr><td colspan="5">GRUPO DE TRABAJO DE AUDITORÍA:</td></tr>
<tr><td colspan="2">Nombre</td><td>Cargo</td><td colspan="2">Especialización</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">FECHA DE INICIO DE LA AUDITORÍA:</td><td colspan="2"></td></tr>
<tr><td colspan="3">FECHA DE FINALIZACIÓN DE LA AUDITORÍA:</td><td colspan="2"></td></tr>
<tr><td colspan="5">HERRAMIENTAS UTILIZADAS:</td></tr>
<tr><td colspan="5">ALCANCE:</td></tr>
<tr><td colspan="5">PROCEDIMIENTOS APLICADOS:</td></tr>
</table>

INFORME DE LAS DEBILIDADES DETECTADAS:		
SITUACIÓN ACTUAL	**RECOMENDACIÓN**	**COMENTARIO DE LA GERENCIA DEL ÁREA**
CONCLUSIONES:		
RESPONSABLES:		
Nombre	**Cargo**	**Firma**

Tabla . Formato de informe de la auditoría

Fuente: Autor

3.5. Socialización de la metodología de auditoría desarrollada

Una parte importante de este estudio es dar a conocer a las personas que están relacionadas con TI y específicamente a las que forman parte del área de Calidad de Software de un banco mediano en Ecuador, el tema desarrollado y el resultado que en este caso es una metodología de auditoría. El objetivo es obtener con base a una exposición del

tema al personal del área, una retroalimentación que considere aspectos como el interés, importancia, el grado de aceptación y si puede llegar a ser considerada como una alternativa en caso de requerir una auditoría del área de Calidad de Software, como una herramienta metodológica que ayude a mejorar los sus procesos.

3.5.1. Esquema de socialización de la metodología de auditoría desarrollada

Para que se conozca la metodología desarrollada a un grupo de personas que sean parte del área de Calidad de Software, fue necesario acudir a uno banco mediano del Ecuador en donde se brindó las facilidades para poder informar, difundir y socializar la metodología propuesta.

El banco donde se realizó este proceso fue BanEcuador[1], que tiene entre otras un área de certificación de requerimientos de software (Calidad), y está conformada por 10 personas entre el director y los analistas de calidad. Es a este grupo de personas a quienes se les comparte la información bajo el siguiente esquema.

Se genera una presentación en PowerPoint (Anexo1) cuyo objetivo fue dar a conocer el tema de tesis desarrollado. La parte fundamental del tema es la metodología propuesta para evaluar el Área de Calidad de Software en bancos medianos del Ecuador, que se desarrolla previo a la obtención del título de "Magister en Tecnologías de Información con Mención en Seguridad de Redes y Comunicación".

En esta presentación se incluye el título de la tesis desarrollada, información de los objetivos específicos del tema propuesto. De igual manera se presenta un resumen de causas y el efecto que puede llegar a determinar fallos en los procesos del área, los procesos que se ejecutan en el área y como se llega a determinar los dominios, procesos y objetivos de control de COBIT mediante una relación con los procesos del área de calidad. Y la última parte de la exposición se centra en explicar las fases de la metodología con las herramientas y papeles trabajos que se utilizan para cada fase.

La exposición se realiza en una sala de la propia entidad bancaria y para constancia de la asistencia de los participantes se genera un documento que contiene nombre y apellido, cédula de identidad, email y firma de cada participante; de acuerdo como se muestra en el

[1] Autorizado por Ivan Fonseca, Subgerente de Gestión y Control Tecnológico

Anexo 2 de este trabajo. Se incluye además imágenes que se obtienen del momento en el que se está realizando la presentación Anexo 4.

3.5.2. Determinar el grado de aceptación de la metodología de auditoría desarrolla

Luego de haber realizado la exposición con los datos más importantes relacionados con la metodología de auditoría para el área de Calidad de Software orientada a bancos medianos en Ecuador, con base en el marco de referencia COBIT; se requiere conocer el grado de aceptación que llego a tener en los participantes y si puede ser adoptada o difundida en caso de requerir realizar una auditoría al área de calidad a la que pertenecen.

Para lograr obtener resultados luego de la socialización realizada, se crea una encuesta que contiene un cuestionario cuyo objetivo es conocer el grado de aceptación e importancia que le dan a la metodología, con base en la apreciación de los asistentes a la exposición. Así mismo se recibe los comentarios generados de la mejor manera ya que esto ayudaría a corregir aspectos que no se tomaron en cuenta o que pueden ser cambiados en futuras actualizaciones a la metodología de auditoría desarrollada.

Esta encuesta fue creada mediante la herramienta que ayuda a crear formularios de Google y es enviada a las direcciones de correo de los integrantes del área a los que se les explicó de una u otra manera la metodología desarrollada. Luego de contestar el cuestionario, envían sus respuestas las mismas que son revisadas y tabuladas para generar los resultados que ayudaran a identificar debilidades y aciertos de la metodología socializada.

El formato del cuestionario y las respuestas enviadas por cada participante son verificados en el Anexo 3 de este documento.

3.5.3. Población y Muestra

El quinto objetivo específico de este trabajo es el poder obtener un criterio acerca de la propuesta metodológica que se elabora como tema de tesis. Para lograrlo se envía a una parte de las personas a las que se les dio a conocer la metodología de auditoría al Área de

Calidad de Software, un cuestionario que trata de recoger puntos de vista e impresiones de forma clara y directa sobre el tema.

La población está compuesta por todos los involucrados que recibieron la información por medio de exposiciones, explicaciones individuales y envió de la información a sus direcciones de correo. Para este estudio, se opta por un estudio no probabilístico que permite tomar un segmento de la población basado en un juicio subjetivo sin ningún tipo de formulaciones.

La muestra se distribuye con base en el rol que desempeñan dentro del área de la siguiente manera:

Rol	Cantidad
Analista de calidad	5
Especialista de calidad	2
Coordinador de calidad	3
Director del Área	0
Total:	**10**

Tabla .- Muestra

Fuente: Autor

3.5.4. Resultados de la encuesta realizada sobre la metodología de auditoría propuesta

Los datos obtenidos mediante la aplicación de una encuesta que contiene un cuestionario que recoge información general de la persona encuestada e información relevante, valorando el interés que puede llegar a tener la metodología de auditoría propuesta para cada persona.

Obtención de información general de los encuestados. - La primera parte de la encuesta está enfocada a la obtención de información que ayude a interpretar y reforzar positiva o negativamente, la evaluación a la metodología de auditoría al Área de Calidad de Software a la que los encuestados pertenecen.

De acuerdo con las respuestas logradas, se determina de forma general que, de las 10 personas encuestadas, 8 tienen una profesión relacionada con sistemas y 2 al área de

finanzas. Esto indicaría que se puede llegar a un buen entendimiento del tema explicado ya que las personas están relacionadas o conocen de lo que se propone.

En cuanto a la distribución de roles, según el resultado generado, se tiene que 5 de las 10 personas encuestadas son Analistas de pruebas (Ejecutores de los procesos del área), 3 son coordinadores de pruebas (Gestionan el correcto desenvolvimiento de las actividades que se ejecutan en el área) y 2 son especialistas de pruebas (Conocen detalladamente un módulo o funcionalidad especifica). Proporcionando una mejor perspectiva de los resultados de esta encuesta al ser más los analistas de pruebas y teniendo en cuenta que son quienes ejecutan todos los procesos que son parte del área de Calidad.

Otro dato importante para tomar en consideración es el tiempo de trabajo de cada persona encuestada en temas relacionados con el aseguramiento de la calidad. Según el resultado obtenido a esta interrogante, un 5 de los 10 encuestados trabajan más de 5 años en temas de Calidad de Software, lo que indica que conocen muy bien la problemática del área, y pueden valorar el hecho de tener un mecanismo de detección de los problemas presentes.

Obtención de información para valorar la metodología. - La segunda parte de la encuesta se enfoca en preguntas directas, que pretenden determinar la importancia que puede llegar a tener la metodología propuesta, así como la aceptación de esta herramienta para encontrar falencias en los procesos del área.

Al preguntar sobre la importancia de tener una metodología que ayude a evaluar el área de Calidad de Software en entidades financieras, de forma casi categórica se da la apertura por parte de los encuestados para poder presentar la metodología, ya que representa un beneficio el hecho de poder conocer las debilidades en los procesos que se ejecutan en área considerándose este un aporte positivo.

Para la interrogante planteada de si a la dirección del área o de la organización le interesaría utilizar la metodología de auditoría propuesta de requerir evaluar los procesos del área, los encuestados no ven problema en que en la organización pueda adoptar, como herramienta, una metodología que audite específicamente al área de Calidad de Software y más bien advierten que puede ser una propuesta interesante, que va a generar valor al conseguir resultados específicos solo de los procesos del área.

La interrogante de si la metodología cubre las expectativas acerca de cómo se debe auditar al área de Calidad de Software; los encuestados casi en su totalidad están de acuerdo en que, si se llegará a cubrir con lo requerido para auditar el área, sin embargo, puede existir pequeñas dudas al no haber sido puesta en práctica la metodología propuesta.

Otra inquietud que se busca saber es si la persona que hace parte del área llegaría a utilizar la metodología que fue socializada, alcanzando un resultado muy optimista que presume el entendimiento de los objetivos que se desea lograr, lo que no impidió que se generen observaciones como el no haber incluido la identificación y evaluación de riesgos dentro de los procedimientos a seguir para la auditoría.

De igual manera se necesitó conocer, si los integrantes del área harían una difusión a otras personas o áreas para dar a conocer información acerca de la estructura y diseño de la metodología propuesta y que es lo que se pretende lograr con la aplicación de esta. Se obtiene como resultado que en su mayoría lo harían, considerando que puede servir de apoyo o guía si se necesita determinar fallas en los procesos de cualquier área.

A la interrogante de si encuentra la metodología de auditoría propuesta fácil de aplicar, los participantes de la encuesta, integrantes del área de Calidad de Software, expresan en su mayoría que potencialmente perciben que puede ser de fácil aplicación. Sin embargo, existe el deseo de conocer más acerca de los detalles que pueden llegar a ser importantes, una vez puesta en práctica en un proceso de auditoría.

Y la última interrogante busca determinar si es significativo el desarrollo de este trabajo de tesis. Con base en el resultado se puede deducir que es importante para los encuestados el haber planteado como tema de tesis, el diseño de una metodología de auditoría informática al área de Calidad de Software de entidades financieras.

Las respuestas al cuestionario planteado en la encuesta se encuentran en el Anexo 2 de este documento.

CAPÍTULO IV

CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

4.1. Conclusiones

- En esta investigación se logró obtener información de como opera el área de Calidad de software y parte de la problemática existente debido a falencias que son descritas por el personal que hace parte del área. Esta descripción da un sustento para generar la metodología propuesta, puesto que hay la necesidad de conocer de forma específica mediante una auditoría, los problemas que presentan directamente a los procesos que hacen parte del área. Además, se analizan trabajos investigativos que se orientan a evaluar el entorno de Calidad de Software de forma general. En algunos casos los autores para el desarrollo de sus investigaciones se basan en estándares ya establecidos como el Marco de Referencia COBIT, ITIL V3, el estándar ISO 9001/2000 pero los que interesan son los que utilizan COBIT como guía y base para el diseño de una metodología.

- El resultado de esta investigación define una metodología de auditoría dirigida a bancos privados medianos en Ecuador, con la ayuda del Marco de referencia COBIT cuyo objetivo, una vez aplicada, es identificar los procesos que pueden tener deficiencias. Para conseguirlo se realiza un mapeo de los componentes de COBIT con los procesos del Área de Calidad de Software que se consideran similares y que pueden ser generales para las entidades financieras medianas en Ecuador; llegando a obtener como resultado nueve objetivos de control que son parte de cuatro procesos de dos dominios de COBIT, que son los cubren la evaluación de los procesos que se ejecutan en el área.

- El modelo metodológico diseñado, planteó utilizar un esquema de recolección de información mediante entrevistas, que se utilizan para detallar los antecedentes que

hacen parte del plan del plan de auditoria y que se presentan como una guía a seguir en la etapa de ejecución. Se complementó con la inclusión de cuestionarios que son los utilizados para obtener información, que luego de acuerdo con el análisis que se realice, pretenden dar a conocer el nivel de madurez en el que se encuentra cada proceso del área y que se entregan de forma resumida en un informe final de resultados.

- Como parte de los objetivos de la investigación se planteó la necesidad de socializar el trabajo realizado. Para conseguir cumplir con este objetivo se planificó presentaciones tanto grupales como personales, donde se explicó de forma resumida como se desarrolló esta propuesta metodológica, cuáles son sus fases y como se podría aplicar cuando se ejecute una auditoría al área de Calidad de Software.

- Para conocer el grado de aceptación de la metodología propuesta, se utilizó como instrumento un muestreo no probabilístico, aplicado a un grupo de personas que participaron de la socialización y que son parte del área de Calidad. Este muestreo genera una opinión de aceptación, que por la orientación cualitativa de la misma se perfila como aceptable, sin embargo, existen observaciones a tomar en cuenta para futuros trabajos como el hecho de tener un ejemplo de aplicabilidad de esta, donde se genere resultados, así como el manejo de riesgos que no se contempló en el diseño de esta metodología de auditoría.

4.2. Recomendaciones

- Se recomienda que el método utilizado para identificar los procesos y la relación que existe con los dominios de COBIT, sea utilizado para futuros desarrollos metodológicos ya que se basa en un análisis de buenas prácticas.

- En vista de que esta metodología facilitaría la identificación y diagnóstico en los procesos del Área de calidad de Software para entidades financieras en Ecuador, se recomienda aplicarla no solo en entidades financieras medianas sino también en entidades financieras pequeñas que cuenten con un área destinada a realizar pruebas de nuevos desarrollos de software con el fin de conocer similitudes, diferencias y limitaciones que presentan dichas entidades en el manejo de sus procesos.

- Se recomienda que previo a la aplicación de la metodología propuesta, se emita una charla para dar a conocer la metodología a utilizar y además se incluya información sobre el Marco de referencia COBIT al personal que participará de la auditoría, con el fin de garantizar el entendimiento de esta.

- Un aspecto importante que se recomienda tomar en consideración es que cuando se aplique la metodología de auditoría propuesta, se cuente con un equipo multidisciplinario integrado con por lo menos dos personas del área que interactúen durante todo el proceso de auditoría. Puede ser el director y una persona que conozca de los procesos del área y que este presto en todo momento a colaborar cuando se lo requiera con el fin de conseguir resultados apegados a la realidad.

- La Gerencia, Dirección o Coordinación de TIC en todo momento debe permanecer informada de las novedades presentadas ya que con esto se estaría monitoreando constantemente el desarrollo de la auditoría y se podría garantizar en parte que la metodología propuesta genere al final un informe que sustente los resultados de forma eficiente.

4.3. Trabajos Futuros

- Como trabajo futuro, se plantea elaborar una propuesta que abarque no solo el área de Calidad de Software en entidades financieras medianas en Ecuador; sino que se complemente con la evaluación del al ciclo de vida completo de un producto de software desde el análisis de sus requerimientos hasta la entrega y soporte del producto en producción. Con eso se garantizaría que, en todas las etapas del ciclo de un desarrollo, exista la forma de identificar posibles fallas que deriven en problemas que puedan afectar la continuidad del negocio.

CAPÍTULO V

BIBLIOGRAFÍA

Bahamon, J. (1991). Control de calidad ·en el software. *ICESI*, 42–52. Retrieved from https://repository.icesi.edu.co/biblioteca_digital/bitstream/item/4008/1/Control_calidad_software.pdf

Cabrera, V. (2014). *ATENCIÓN A LAS NECESIDADES DE MICROCRÉDITO EN EL ECUADOR A TRAVÉS DE UNA FORMULACIÓN ESTRATEGICA FOMENTADA POR EL BANCO*. Retrieved from https://repositorio.uide.edu.ec/bitstream/37000/421/1/T-UIDE-0400.pdf

Castro, P., & Alvarez, C. (2018). *Diseño de una metodologia de auditoria para el control de los procesos de pruebas en entidades financieras* (Universidad Catolica de Colombia). Retrieved from http://repository.ucatolica.edu.co:8080/handle/10983/16056

Coronel, K. (2013). *Metodología de evaluación del gobierno, riesgos y cumplimiento de la tecnología de información en instituciones del sistema financiero ecuatoriano*. 120.

Dragomir, R. G. (2017). The Audit of the Quality Control System within the Information Technology Field. *Economic Development, Environment and People*, *6*, 45–54. https://doi.org/10.26458/jedep.v6i2.532

García, J., Amescua, A. De, & Velasco, M. (2006). *TOP 10 de factores que obstaculizan la mejora de los procesos de verificación y validación en organizaciones intensivas en software*. Retrieved from https://www.redalyc.org/pdf/922/92220204.pdf

García, L., & Chiclote, R. (2016). *MODELO DE EVALUACIÓN DEL PROCESO DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN DE LA C.A.C. "CHICLAYO" LTDA. BASADO EN COBIT 5* (UNIVERSIDAD NACIONAL DE TRUJILLO). Retrieved from http://dspace.unitru.edu.pe/handle/UNITRU/10036

García, Palao, M., & De la Calle, J. (2016). *COBIT Una Radiografía del Marco (en su XX aniversario, 1996-2016)*. Retrieved from https://adacsiargentina.files.wordpress.com/2017/06/2017-06-13_itti-isaca-cobit-xx-aniversario_radiografc3ada-de-cobit_v01-00.pdf

Hernández, S., & Lomprey, G. (2008). *La importancia de la calidad en el desarrollo de productos de software*. Retrieved from

http://fit.um.edu.mx/CI3/publicaciones/Technical Report COMP-018-2008.pdf

Institute IT Governance. (2005). *Cobit 4.0 Marco de Referencia*. USA.

Institute IT Governance. (2008). *Alineando Cobit 4.1, ITIL V3 e ISO/IEC 27002*. Retrieved from https://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

ISACA. (2011). *Manual de preparacion al examen CISA 2011*.

ISACA. (2019). *MARCO DE REFERENCIA COBIT: Introducción y metodología* (p. 64). p. 64.

IT Governance Institute. (2007). Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez. *Cobit*, *4.1*, 211. Retrieved from www.isaca.org/cobitfeedback

Moreno, J. J., Bolaños, L. P., & Navia, M. A. (2010). *Exploración de Modelos y Estándares de Calidad Para el Producto Software*. (1), 39–53.

Muñoz, C. (2002). *Auditoria en Sistemas Computacionales* (1st ed.). Pearson Educación de México.

Perry, W. E. (2007). *Effective Methods for Software Testing*. Retrieved from https://books.google.com/books?id=q1WwdUZd7IAC&pgis=1

Piattini, M., & del Peso, E. (2007). *Auditoría Informática Un enfoque práctico*. Mexico: ALFAOMEGA.

Rodríguez, M., & Piattini, M. (2015). *Experiencias en la Industria del Software: Certificación del Producto con ISO/IEC 25000*. 14. Retrieved from http://eventos.spc.org.pe/cibse2015/pdfs/01_IT15.pdf

Sandoval, H. (2012). *Introducción a la Auditoria* (Primera). Retrieved from http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf

Santacruz, J., Vega, C., Pinos, L., & Cárdenas, O. (2017). Sistema cobit en los procesos de auditorias de los sistemas informaticos. *REVISTA CIENCIA E INVESTIGACION*, *2*(8), 65–68. https://doi.org/https://doi.org/10.26910/issn.2528-8083vol2iss8.2017pp65-68

Scalone, F. (2006). *ESTUDIO COMPARATIVO DE LOS MODELOS Y ESTANDARES DE CALIDAD DEL SOFTWARE*. Retrieved from http://laboratorios.fi.uba.ar/lsi/scalone-tesis-maestria-ingenieria-en-calidad.pdf

Suárez, L. (2009). *Proval - Desarrollo de una metodología para la autoevaluación del proceso software en las pequeñas y medianas empresas* (UNIVERSIDAD

TECNOLÓGICA DE LA MIXTEC). Retrieved from http://biblioteca.utm.mx/resultados_dig.php?rconsulta=palabra&cadenat=proval&bbuscar=Enviar+consulta

Superintedencia de Bancos. (2010). *SISTEMA FINANCIERO SUPERINTENDENCIA DE BANCOS* (pp. 1277–1287). pp. 1277–1287. Retrieved from https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2017/06/L1_XXI_cap_II.pdf

Superintedencia de Bancos Portal Estadístico. (2018). *BOL_BP_SEPTIEMBRE 2018*. Retrieved from http://estadisticas.superbancos.gob.ec/portalestadistico/portalestudios/?page_id=415

ANEXO 1

OBJETIVO DE LA PRESENTACIÓN:

Dar a conocer una metodología para evaluar el área de Calidad de Software en bancos medianos del Ecuador, desarrollada como tema de tesis previo a la obtención del titulo de "Magister en Tecnologías de Información con mención en Seguridad Informática"

Para cumplir con este objetivo se desarrollan los siguientes temas:

TEMA PROPUESTO:

"METODOLOGÍA DE AUDITORIA INFORMÁTICA PARA EVALUAR EL ÁREA DE CALIDAD DE SOFTWARE EN BANCOS PRIVADOS MEDIANOS DEL ECUADOR, BASADA EN EL MARCO DE REFERENCIA COBIT"

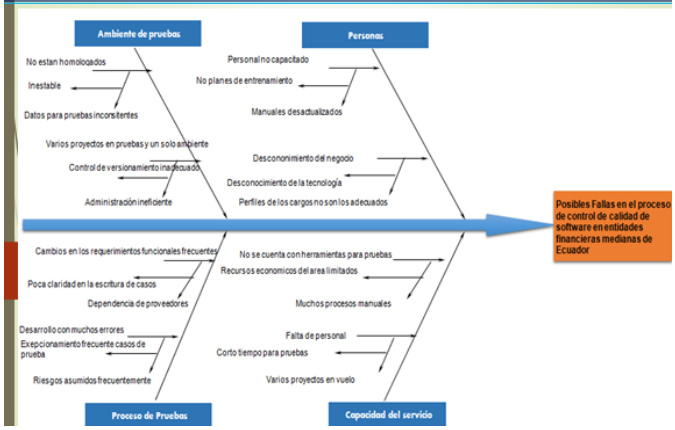
OBJETIVOS:

-Analizar la documentación que se relacione con metodologías, controles, normas que se hayan aplicado para la evaluación de los procesos que se ejecutan en el Área de Calidad de Software, basados en el Marco de referencia COBIT.

-Diseñar una metodología de auditoría informática al Área de Calidad de Software dirigido a bancos privados medianos en Ecuador, con la ayuda del Marco de referencia COBIT.

- Difundir y socializar la metodología con personas que trabajan en el área de calidad de un banco mediano y realizar una encuesta que dé a conocer el grado aceptación de la misma.

DIAGNÓSTICO GENERAL:



PROCESOS DEL ÁREA DE CALIDAD DE SOFTWARE

	BANCO 1	BANCO 2	PROCESOS RELACIÓN
	Diners Club	General Rumiñahui	Bancos medianos del Ecuador
Proceso	Admistrar la Calidad	Control de Calidad	- Los dos bancos comparten los mismos conceptos sobre el proceso de Calidad. - Se diferencian por la forma de adquirir e implementar el proceso, sub procesos y demás actividades a ejecutar en el área. - Dependen de las necesidades y políticas de cada Banco.

PROCESOS DEL ÁREA DE CALIDAD DE SOFTWARE

	BANCO 1	BANCO 2	PROCESOS RELACIÓN
	Diners Club	General Rumiñahui	Bancos medianos del Ecuador
Subprocesos/ Fases	-Estimación y Análisis Pruebas -Planeación de Pruebas -Ejecutar pruebas y seguimiento de incidentes	-Análisis de Requerimientos(Estimación de esfuerzo) -Diseño de Alto y Bajo Nivel(Estrategia de pruebas) -Construcción de las pruebas(Guiones de prueba) -Pruebas de Integración(Rondas de prueba) -Paquete y liberación(Participación en el comité de cambios) -Post Implementación(Soporte para estabilización)	- Existe una clara relación entre las fases o sub procesos de calidad que se ejecutan para cada uno de los bancos analizados. -Se diferencian en la forma en la que cada banco presenta las actividades ya que en algunos casos una actividad se divide en varias actividades pero el resultado debe ser el mismo. - Se identifica que en el Banco 1, no tienen las fases de liberación y post implementación y de lo que se puedo conocer las ejecuta otra área.

DESARROLLO DE LA METODOLOGÍA PROPUESTA:

Relación de los componentes de COBIT con el proceso y actividades del Área de Calidad

COBIT			Meta relacionada con TI:
Dominio:	Proceso:	Objetivo de control:	Evaluación de los procesos del área de calidad de software en entidades financieras medianas en Ecuador
Planear y organizar	PO4 Definir los procesos, organización y relaciones de TI	PO4.7 Responsabilidad de aseguramiento de calidad de TI	Proceso de apoyo que genera el Organigrama del área, roles y responsabilidades de sus integrantes
	PO8 Administrar la calidad	PO8.1 Sistema de administración de calidad	Proceso genérico de apoyo que evalúa la administración de la calidad de los servicios de TI y para este caso de estudio específicamente para el área de Calidad de Software
		PO8.2 Estándares y prácticas de calidad	Se incluye en la ejecución de los procesos del área metodologías, mejores prácticas, estándares, procedimientos y políticas claras de calidad .
		PO8.6 Medición, monitoreo y revisión de la calidad	Proceso de monitoreo y revisión constante del desempeño y mejora continua del cumplimiento de la calidad.

Figura .- Diapositivas de la presentación para socialización de la metodología

Fuente: Autor

ANEXO 2

REGISTRO DE ASISTENTES A LA SOCILAIZACIÓN

UNIVERSIDAD INTERNACIONAL SEK ECUADOR SER MEJORES	LISTADO DE ASISTENTES A LA SOCIALIZACIÓN DEL TEMA: "METODOLOGÍA DE AUDITORIA INFORMÁTICA PARA EVALUAR EL AREA DE CALIDAD DE SOFTWARE EN BANCOS PRIVADOS MEDIANOS DEL ECUADOR, BASADA EN EL MARCO DE REFERENCIA COBIT"

Expositor	Ing. Henry Vargas García		
Lugar	Instalaciones de la entidad financiera BanEcuador		
Fecha	12-03-2019	**Hora inicial**	17h00

El registro de esta información se utilizará con fines didácticos y pedagógicos.

Ítem	Nombre completo	Cédula de identidad	Email	Firma
1	Ma. Jessenia Alvarado V.	1715317145	jessenia.alvaradot.77@gmail.com	
2	Iván Fonseca	1714325907	ivan.fonseca@banecuador.fin.ec	
3	Verónica Almeida	1713745279	veronica.almeida@banecuador.fin.ec	
4	Iván Veloz	0602914525	ivan.veloz@banecuador.fin.ec	
5	HORACIO PILLASTO	0916749326	moragpillajo@hotmail.com.	
6	Alexandra García	1718687542	alaxagarcia@hotmail.com.ar	
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Observaciones:

Figura .- Registro de asistentes a la socialización de la metodología propuesta

Fuente: Autor

ANEXO 3

FORMATO DE ENCUESTA

Evaluación de la metodología de auditoría propuesta

El objetivo de esta encuesta es conocer el grado de aceptación e importancia que puede llegar a tener la Metodología de auditoría propuesta para evaluar el área de Calidad de Software en bancos medianos del Ecuador, basada en el Marco de referencia COBIT y que se desarrolla como tema de tesis previo a la obtención del título de "Magister en Tecnologías de Información con mención en Seguridad de redes y comunicación" en la Universidad Internacional Sek (UISEK).

*Obligatorio

Datos para la encuesta

La información registrada en esta encuesta es de carácter confidencial y únicamente será utilizada con fines académicos

Nombre y apellido *

Tu respuesta

Ingrese su dirección de correo electrónico

Tu respuesta

¿Su profesión se relaciona con alguna de las siguientes opciones? *

- ○ Sistemas
- ○ Finanzas
- ○ Administración
- ○ Otra

¿Cuál es su rol dentro del área? *

- ○ Analista de pruebas
- ○ Especialista de pruebas
- ○ Coordinador de pruebas

¿Cuál es su rol dentro del área? *

- ○ Analista de pruebas
- ○ Especialista de pruebas
- ○ Coordinador de pruebas
- ○ Dirección del área

¿Cuánto tiempo trabaja en temas relacionados con aseguramiento de la calidad? *

Elegir

¿Cree importante tener una metodología que ayude a evaluar el Área de Calidad de software en una entidad financiera? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

¿Le puede interesar a la Dirección de una entidad financiera utilizar la metodología de auditoría propuesta, si se requiere realizar una auditoría del área de Calidad de software? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

¿La metodología propuesta cubre las expectativas acerca de cómo se debe auditar al Área de Calidad de Software? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

¿Usted llegaría a utilizar esta metodología de auditoría de requerirlo? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

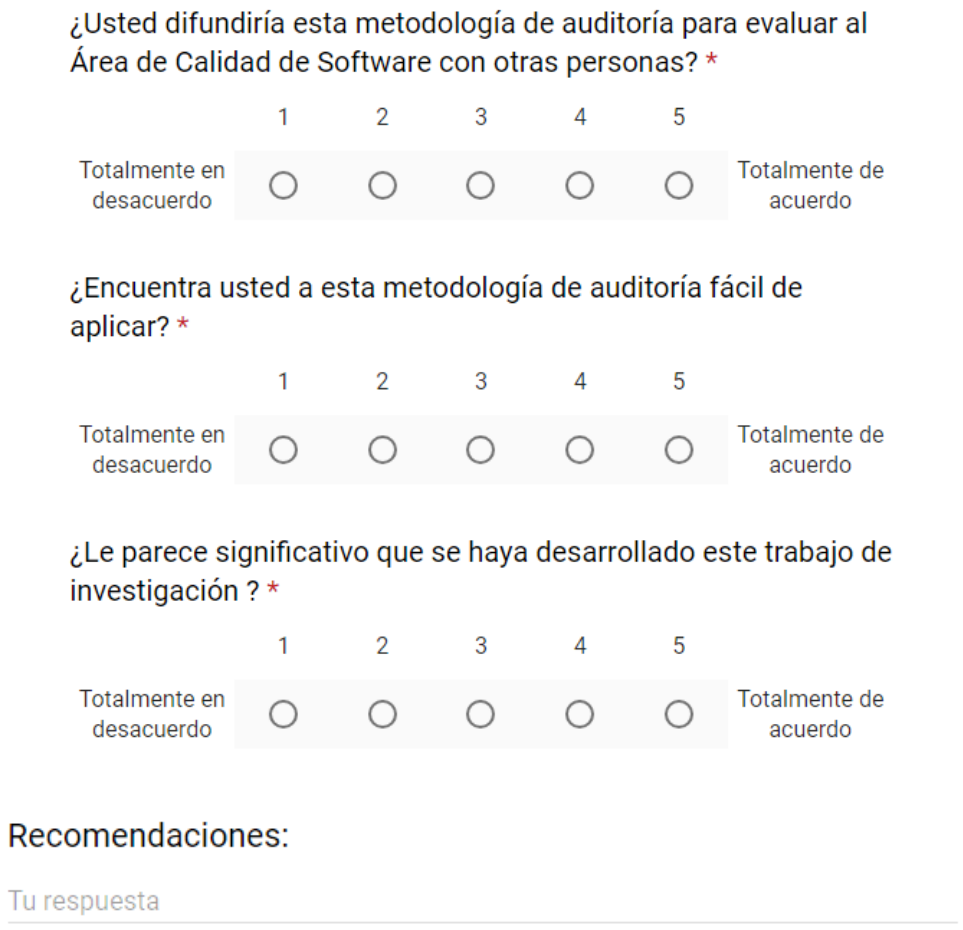
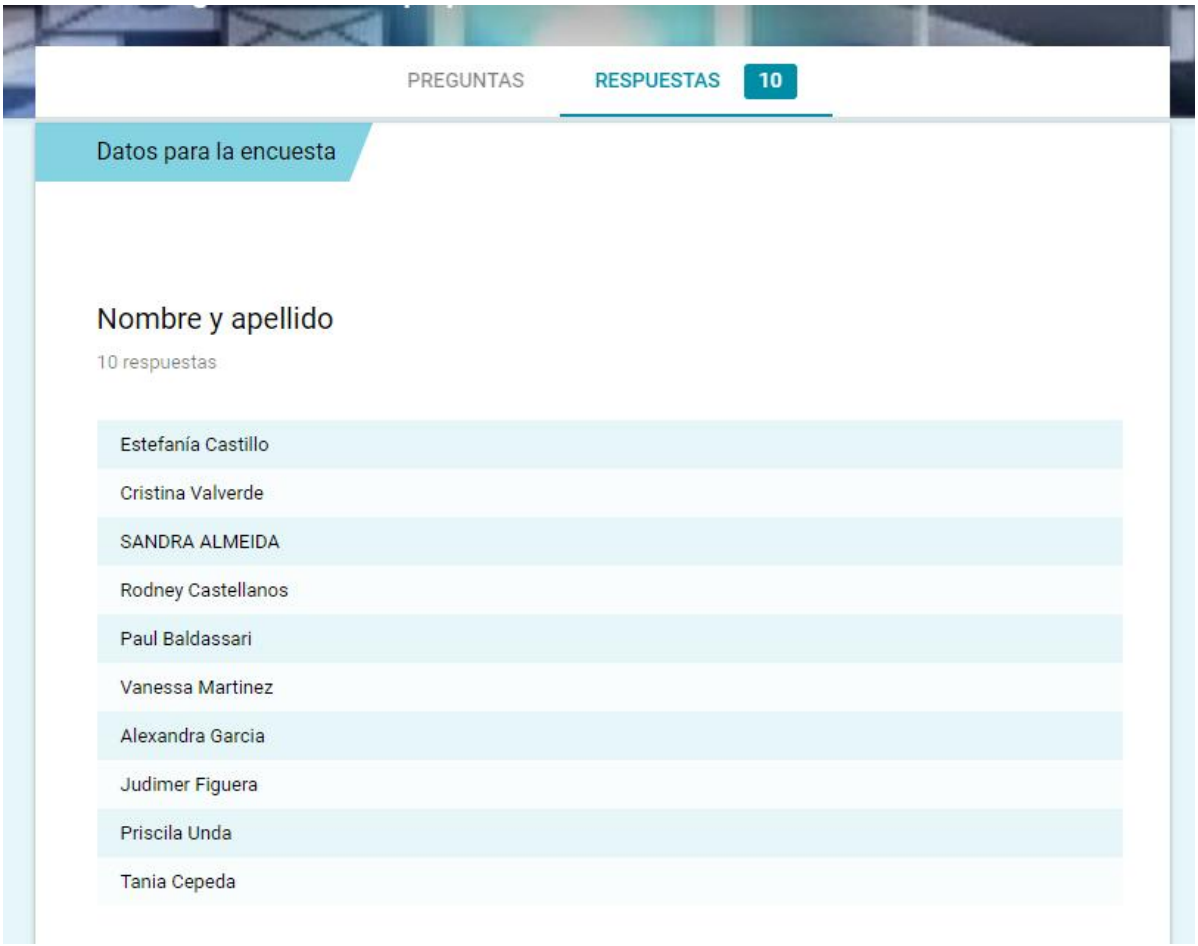


Figura .- Formato de encuesta para evaluar la metodología de auditoría propuesta.

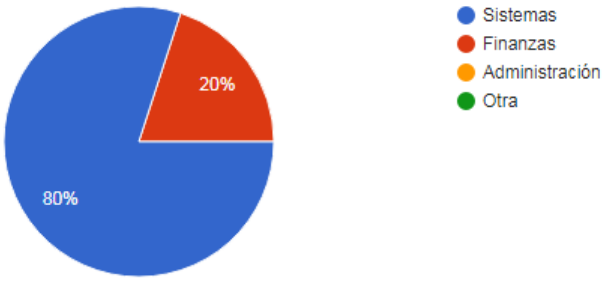
Fuente: Autor.

PRESENTACIÓN DE RESULTADOS



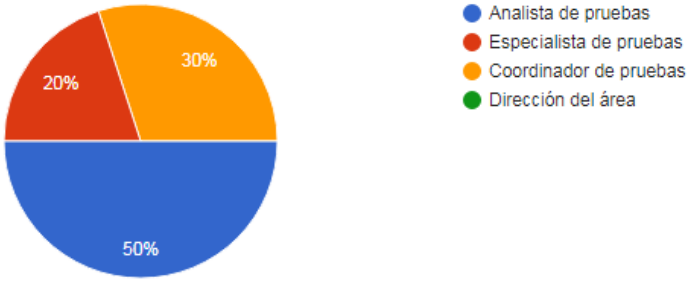
¿Su profesión se relaciona con alguna de las siguientes opciones?

10 respuestas



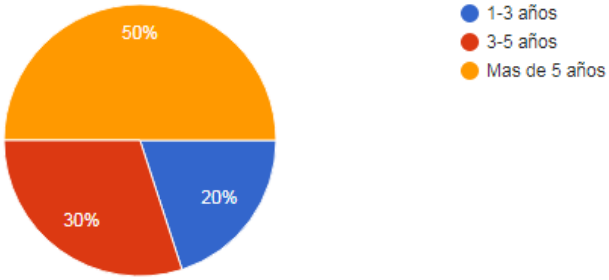
¿Cuál es su rol dentro del área?

10 respuestas



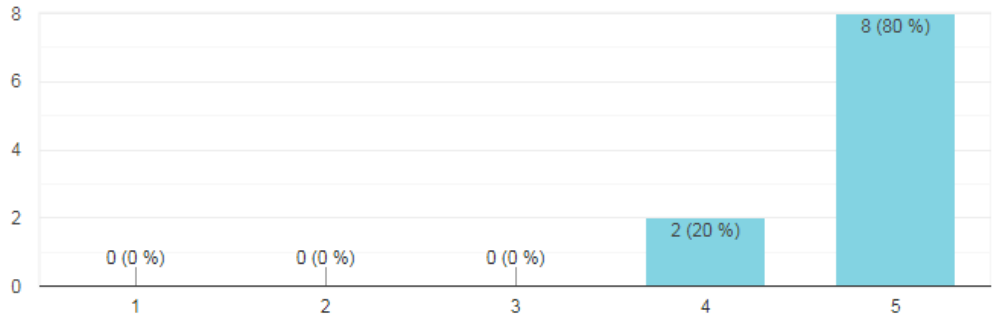
¿Cuánto tiempo trabaja en temas relacionados con aseguramiento de la calidad?

10 respuestas



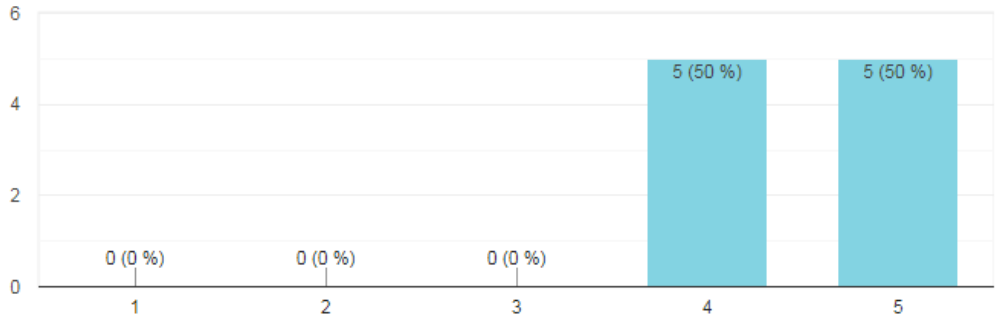
¿Cree importante tener una metodología que ayude a evaluar el Área de Calidad de software en una entidad financiera?

10 respuestas



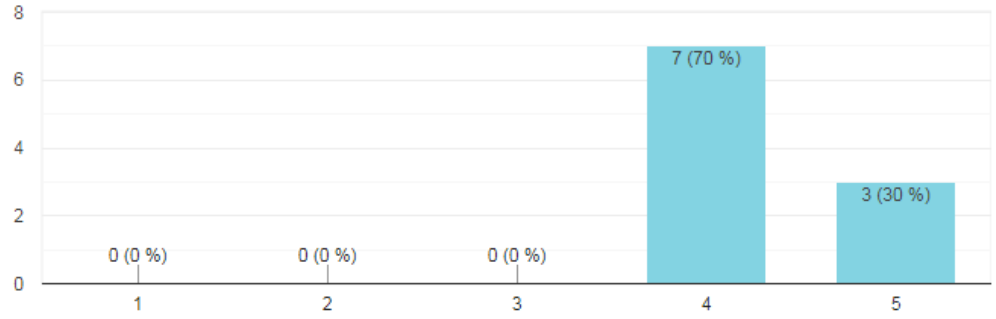
¿Le puede interesar a la Dirección de una entidad financiera utilizar la metodología de auditoría propuesta, si se requiere realizar una auditoría del área de Calidad de software?

10 respuestas



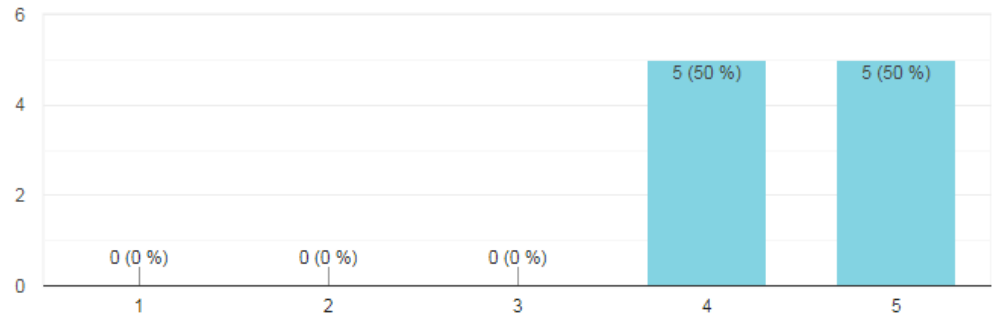
¿La metodología propuesta cubre las expectativas acerca de cómo se debe auditar al Área de Calidad de Software?

10 respuestas



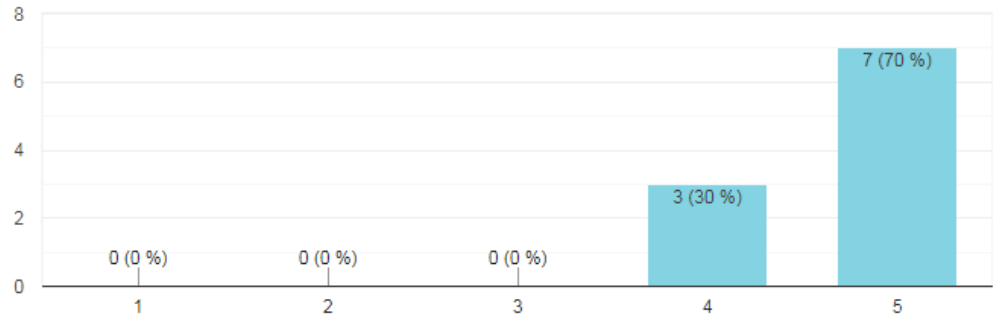
¿Usted llegaría a utilizar esta metodología de auditoría de requerirlo?

10 respuestas



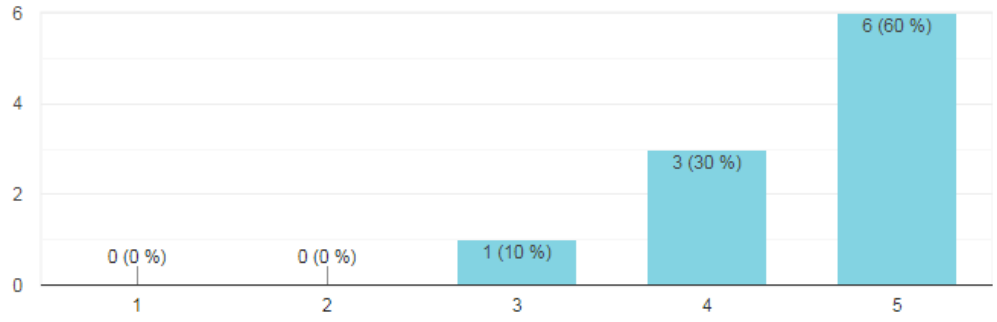
¿Usted difundiría esta metodología de auditoría para evaluar al Área de Calidad de Software con otras personas?

10 respuestas



¿Encuentra usted a esta metodología de auditoría fácil de aplicar?

10 respuestas



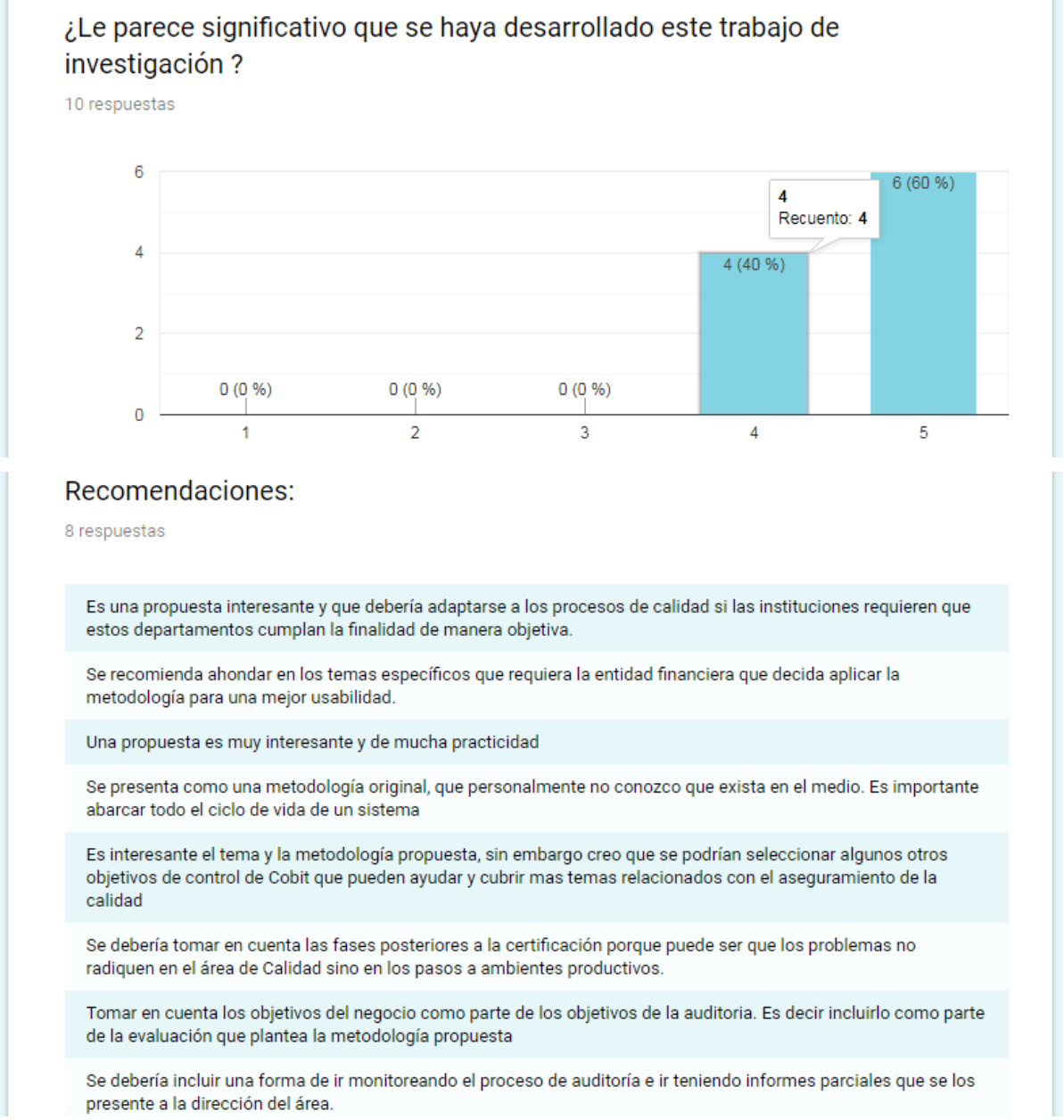


Figura .- Resultados de la encuesta para determinar la aceptación de la metodología propuesta.

Fuente: Autor

ANEXO 4

EVIDENCIAS DE LA DIFUSIÓN, SOCIALIZACIÓN DE LA ENCUESTA

Figura .- Presentación del tema en el Área de Calidad del Banco BanEcuador

Fuente: Autor

Figura .- Presentación del análisis de causa y efecto de una entidad financiera en Ecuador

Fuente: Autor

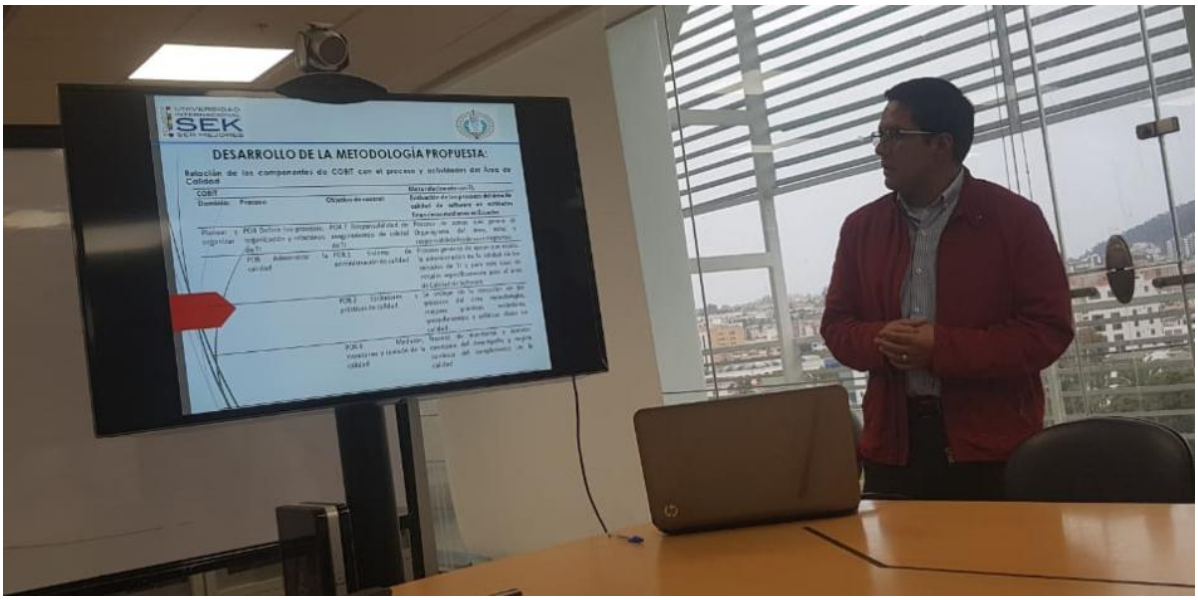


Figura .- Presentación de la relación de los dominios de COBIT con los procesos del Área

Fuente: Autor

Figura .- Presentación de las fases de la metodología propuesta

Fuente: Autor

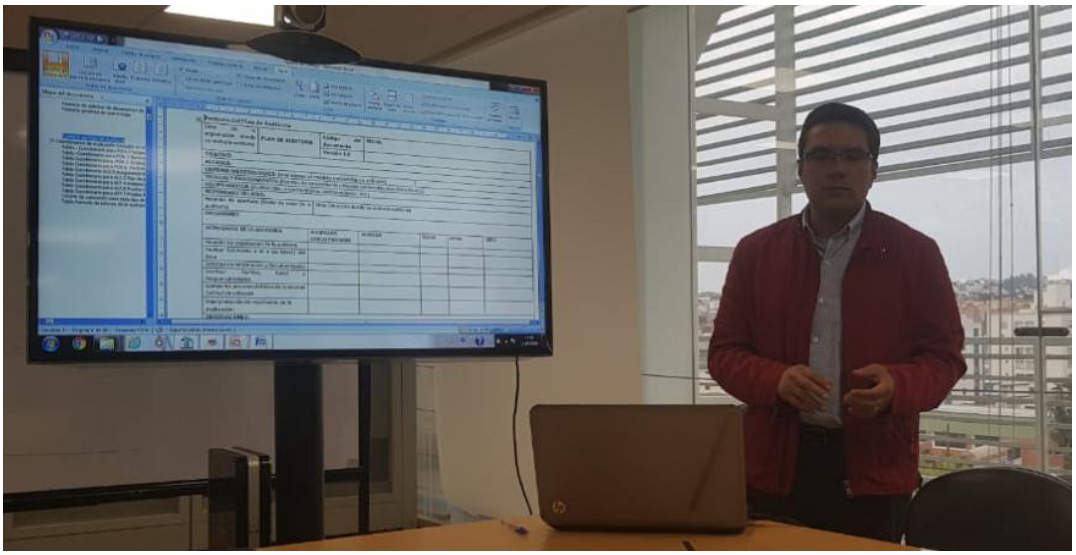
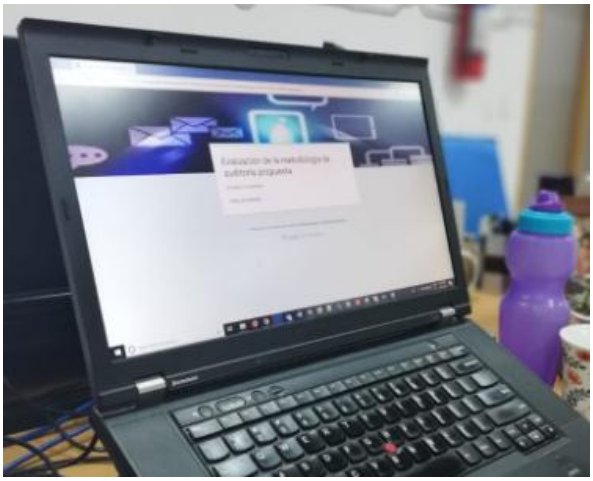
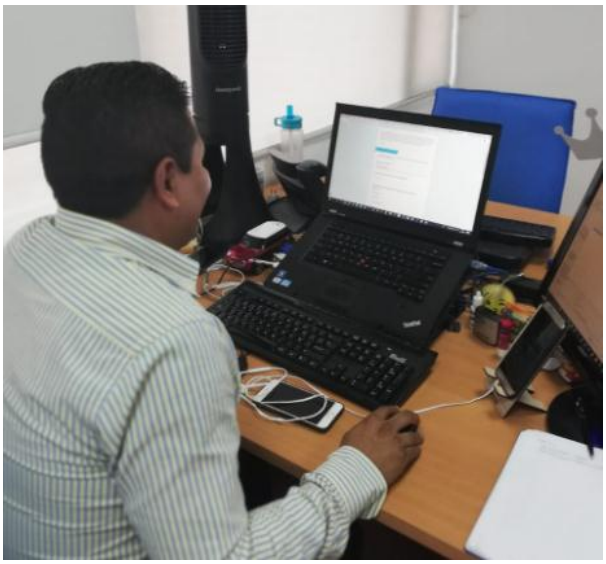


Figura .- Presentación de las herramientas de trabajo (Encuestas, Entrevistas, Cuestionarios, etc.)

Fuente: Autor

EVIDENCIAS DE LA EJECUCIÓN DE LA ENCUESTA





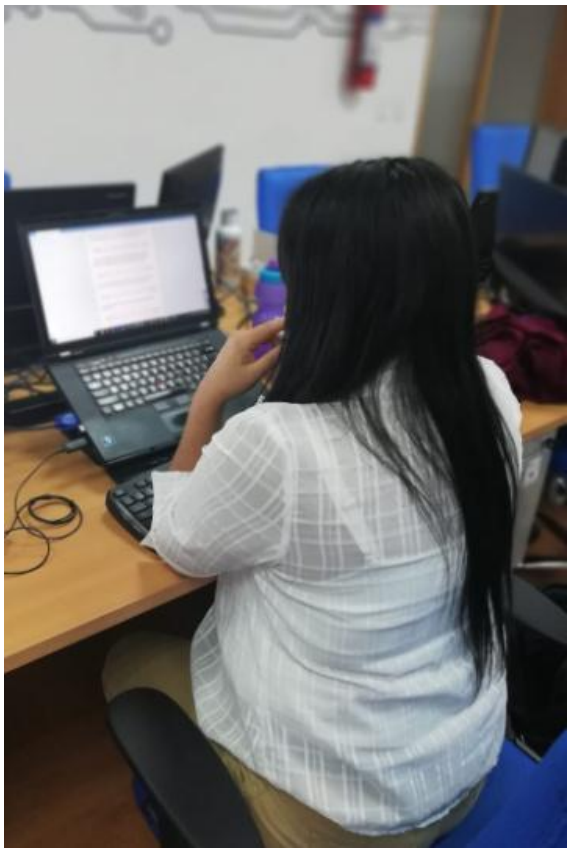


Figura .- Integrantes del área de Calidad, llenado de la encuesta luego de la explicación del tema

Fuente: Autor