GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011 ADAPTANDO LA METODOLOGÍA COBIT 5 AL CASO DE ESTUDIO: PROCEDIMIENTO RECAUDOS DE LA DIVISIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA.

MILENA NATALIA CRUCES CERÓN

JUAN PABLO MORA PALACIOS

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Sistemas

Grupo de Tecnologías de la Información (GTI)

Popayán, Julio de 2016

GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011 ADAPTANDO LA METODOLOGÍA COBIT 5 AL CASO DE ESTUDIO: PROCEDIMIENTO RECAUDOS DE LA DIVISIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA.

Trabajo de Grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

MILENA NATALIA CRUCES CERÓN

JUAN PABLO MORA PALACIOS

Director: Esp. Siler Amador Donado

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Sistemas

Grupo de Tecnologías de la Información (GTI)

Popayán, Julio de 2016

Tabla de contenido

Lista de ilustraciones.

Lista de Tablas.

RESUMEN

En este trabajo se presenta la fase plan de un Sistema de Gestión de la Seguridad de la Información (SGSI) [1], según la norma NTC-ISO/IEC 27001 [2], adaptando la metodología COBIT 5 [3] para la valoración del riesgo en el procedimiento de recaudos de la División de Gestión Financiera de la Universidad del Cauca. A continuación se desarrolla un marco conceptual y metodológico del sistema de gestión siguiendo la perspectiva del estándar ISO 27001:2005; posteriormente se presenta la metodología, la cual fue escogida teniendo en cuenta fuentes consultadas que revelaron la importancia para su implementación en el desarrollo de este trabajo; se destacan el alcance, identificación de activos, análisis, evaluación del riesgo y selección de controles y objetivos de control.

PLANTEAMIENTO DEL PROBLEMA

El área de Recaudos de la división financiera de la Universidad del Cauca se encarga de reconocer, relevar, controlar y garantizar, el recaudo y los registros de los recursos financieros a los cuales la universidad tiene derecho, los cuales se encuentran enmarcados en la normatividad bancaria, presupuestal y contable vigente. Se requiere proteger la entidad de las diferentes amenazas que en algún momento podrían generar un riesgo el cual se traduciría en pérdidas a nivel de información, servicio o financiero.

Actualmente, la institución no cuenta con un SGSI que permita gestionar los riesgos en la Seguridad de la Información, lo que dificulta establecer y visualizar el estado global se la seguridad por lo que no hay una plena identificación o adecuación de controles basados en una evaluación de riesgo y medición de los mismos.

La Universidad del Cauca ha iniciado un proceso para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo como recomendación la norma ISO/IEC 27001:2013. “Cuando se va a implementar un SGSI en una organización, se debe seleccionar una metodología de gestión de los riesgos apropiada para la organización para que esta haga una identificación y clasificación de sus activos de información y para la valoración y tratamiento de riesgos”

En este trabajo de grado se evaluará y adaptará el Marco Cobit 5 para Riesgos como metodología para la valoración y gestión del riesgo en el caso de estudio propuesto, con el objetivo de fortalecer integralmente la entidad y mejorar los pilares fundamentales de la seguridad correspondiente a la Integridad, Confidencialidad y Disponibilidad de la información garantizando la debida protección de la información del negocio y la privacidad de la información de sus partes interesadas.

DIAGNOSTICO DEL PROBLEMA

Las organizaciones deben llevar a cabo valoraciones de riesgo de la seguridad de la información, deben conservarla documentada y planificar intervalos de actualización para de esta manera medir la eficacia del sistema de gestión de seguridad de la información; a partir de lo anterior surge el siguiente interrogante:

¿Por qué es necesaria una metodología de análisis de riesgo?

Un análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto sobre nuestro proyecto, si este es mal elaborado o no sigue una metodología adecuada puede suponer el desperdicio de todos los esfuerzos para proteger los activos, desde una elección de controles de seguridad que no se ajusten a las necesidades de las empresa hasta un plan mal establecido y que no dé solución a un evento dado.

La metodología nos ayuda a valorar el riesgo y determinar el valor de los activos de información identificando las amenazas, riesgos y las vulnerabilidades que existen, también determina las consecuencias potenciales y finalmente prioriza los riesgos derivados y clasificándolos en términos de posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo, de esta forma se puede medir por ejemplo la pérdida económica, la reputación de la empresa entre otros. Una vez se tenga esta evaluación se debe afrontar el riesgo aceptándolo, transfiriéndolo, mitigándolo o evitándolo con la ayuda de los controles.

INTRODUCCIÓN

Actualmente, el Plan Vive Digital [4], liderado por el Ministerio de las Tecnologías de la información y las comunicaciones en Colombia (MinTIC), da a conocer las necesidades de aceptar la seguridad informática como un factor primordial para la aprobación de las TIC, por lo cual se convierte en un factor importante a tener en cuenta en la utilización de las nuevas tecnologías para la seguridad de la información para la prestación de servicios. Además, como apoyo a esta iniciativa se presenta la estrategia de Gobierno en Línea [5] que contribuye con la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de las TIC.

La gestión de riesgos constituye un proceso complejo pero necesario dentro de una entidad, las organizaciones necesitan un plan de análisis de valoración del riesgo en la seguridad de la información para garantizar la buena administración.

Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de esta, la persona encargada de su diseño e implementación conjuga un sinnúmero de herramientas y conceptos de ramas como: la estadística, matemáticas, auditoría, administración entre otras.

El presente documento pretende esquematizar y dar a conocer paso a paso como determinar la adaptación e integración de una metodología de valoración de riesgo basada en Cobit 5 para riesgos a la fase de plan de un Sistema de Gestión de Seguridad de la Información según NTC ISO/IEC 27001 en la División de Gestión financiera, específicamente en el área de Recaudos de la Universidad del Cauca

OBJETIVOS

Objetivo General

Desarrollar la fase plan de un sistema de gestión de seguridad de la información según la norma NTC-ISO/IEC 27001, adaptando la metodología COBIT 5 para la valoración del riesgo en la División Financiera de la Universidad del Cauca.

Objetivos Específicos.

- Elaborar el diagnóstico, establecer el alcance, preparar el diseño y el plan de implementación del sistema de gestión de la seguridad de la información (SGSI) con base en la norma ISO/IEC 27001 para la aplicación de la metodología COBIT 5.

- Desarrollar la fase de plan del SGSI, según la norma ISO/IEC 27001 para determinar el análisis de seguridad de la información de la división financiera de la Universidad del Cauca.

- Adaptar la metodología COBIT 5 como mecanismo para la valoración del riesgo con base en la norma ISO/IEC 27001, siguiendo la ISO/IEC 27003[8] como guía de implementación.

- Calibrar y ajustar el mecanismo para la valoración del riesgo a partir de los resultados obtenidos al aplicar la metodología al caso de estudio y formular estrategias de mejora.

1. MARCO TEORICO.

1.1. ¿QUÉ ES UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información, además de mantener la confidencialidad, la integridad y la disponibilidad de la misma ante los miembros y las distintas partes interesadas en la institución.

- Confidencialidad, hace referencia a la información por la que se tiene la certeza de que esta solo puede ser accedida (vista y entendida), por el personal quien tiene la necesidad de ello y ha sido autorizado por el propietario de la misma.
- Integridad, es la información por la que se tiene la certeza de que esta es exacta y completa, la cual no ha sido alterada en modo alguno.
- Disponibilidad, implica a la propiedad de la información por la que se tiene la certeza de que los autorizados a acceder a ella lo pueden hacer cuando lo requieran en todo momento y circunstancia.

La preservación de la confidencialidad, la integridad y la disponibilidad en una empresa son de gran importancia, debido a la competitividad que existe en las organizaciones, las cuales están obligadas a implementar un sistema de gestión de seguridad de información que permita identificar qué quiere ser protegido, y porque, de qué debe ser protegido y como protegerlo.

Para lograr una adecuada seguridad de la información es fundamental contar con el acuerdo y el compromiso de todos los involucrados, un respaldo de los niveles directivos dentro de la entidad y ser conscientes de los beneficios que se puede obtener en una cultura de seguridad, y también del impacto por la materialización de riesgos que no se controlan y están asociados al tema de seguridad de la información.

1.2. NATURALEZA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Durante años, la problemática de las diferentes organizaciones ha sido la seguridad de la información, debido a que todas las empresas creen tener un sistema de seguridad de la información que funciona con eficiencia y eficacia. Sin embargo, lo único que suelen hacer las empresas, frente a la seguridad de

información es actuar de manera reactiva, rara vez se actúa de manera proactiva, esto con el fin de asumir todo el control, lo que implica la toma iniciativa en el desarrollo de acciones creativas y audaces para generar mejoras en un sistema de seguridad de la información.

En el siglo XXI, cuando la gestión del conocimiento es una característica vital en las empresas, se debiera tener formas de poder minimizar el riesgo de que la información se fugue, se altere o simplemente no esté disponible cuando se requiera. Con el fin de proporcionar un marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000. Estas normas van a permitir disminuir el impacto de los riesgos sin necesidad de hacer grandes inversiones en software y la contratación de personal. Para la protección de la información en las empresas, se hace uso del estándar ISO/IEC 27001 el cual está basado en un enfoque de riesgos del negocio, para establecer, implantar, operar, monitorear, mantener y mejorar la seguridad de información; el sistema de gestión incluye, estructura organizacional, políticas, planeación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

1.3. ESTÁNDARES Y NORMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La organización Internacional de Estándares ISO, se originan en la Federación Internacional de Asociaciones Nacionales de Normalización, su finalidad principal es la de promover el desarrollo de estándares internacionales y actividades relacionadas incluyendo la conformidad de los estatutos para la facilitar el intercambio de bienes y servicios en todo el mundo.

Las normas ISO ofrecen soluciones y brinda beneficios para casi todos los sectores de diferente actividad como lo es la agricultura, construcción, ingeniería mecánica, fabricación, distribución, transporte, medicina, dispositivos, tecnologías de información y comunicación, etcétera.

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (comisión internacional de electrónica), la cual tiene algunas similitudes a la familia de las normas de gestión de calidad ISO 9000. Cada una de las normas 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas.

A continuación se definen la temática de cada una de las normas ISO 27000:

- Norma ISO 27000: Gestión de la seguridad de la información (Fundamentos y Vocabulario).

  Esta norma fue contempla en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de la seguridad de la información (SGSI), una descripción del ciclo PDCA (Planificar, Hacer, Verificar y Actuar), al igual que las definiciones de los término que se emplean en toda la serie 27000.

- Norma ISO 27001 Especificaciones de un SGSI.

  Enmarca los requisitos y/o especificaciones del sistema de Gestión de Seguridad de la Información. Esta norma es la norma certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas.

  El ciclo PDCA [9], también conocido como ciclo de mejora continua o ciclo Deming. Esta metodología describe cuatro pasos esenciales que se deben llevar a cabo para la mejora continua de calidad. El ciclo Deming está compuesto por cuatro etapas, de forma de que se termine la cuarta etapa se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para hacer y examinar nuevas mejoras. La aplicación de esta metodología está enfocada para ser usada en empresas y organizaciones.

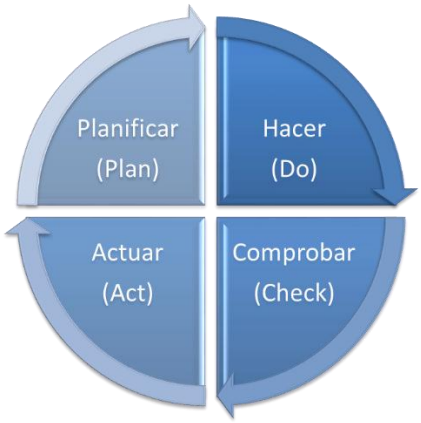

Ilustración 1: Ciclo Deming o ciclo PDCA

Fuente: Propia

La ilustración 1, muestra las cuatro etapas, las cuales son:

- ✓ Planificar (Plan): en esta etapa busca las actividades susceptibles de mejora y establece los objetivos a alcanzar.
- ✓ Hacer (Do): se realizan los cambios para implantar la mejor propuesta.
- ✓ Controlar o verificar (Check): una vez implantada la mejora, se deja un periodo de prueba para determinar si está en su correcto funcionamiento.
- ✓ Actuar (Act): una vez terminado el periodo de pruebas, se procese a estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si el análisis de los resultados son satisfactorios se implantara la mejora de forma definitiva, y si no lo son habrá que decidir si se realiza cambios para ajustar los cambios de resultados o si los rechaza. Una vez terminado la cuarta etapa se procede a volver a la primera etapa periódicamente para estudiar nuevas mejoras a implantar.

En Colombia a través del Instituto Colombiano de Normas Técnicas y Certificación (INCONTEC).

- ISO 27002 [10] Códigos de buenas prácticas.

  Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información; la ISO 27002 contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

- ISO 27003 Guía de implementación del SGSI.

  Esta norma no es certificable y proporciona una guía que contempla todos los aspectos necesarios para el diseño e implementación de un SGSI de acuerdo a la norma certificable ISO/IEC 27001:2005. El objetivo de esta norma es describir las especificaciones y diseño en el proceso de la implantación del SGSI.

- ISO 27004 Sistema de métricas e indicadores [11].

  Esta norma es una guía que permite determinar la eficacia de la implantación de un SGSI, a través del desarrollo y utilización de métricas y técnicas de medida y los controles o grupos de controles implementados según ISO/IEC 27001.

- ISO 27005 Guía de análisis y gestión de riesgo [12].

  Esta norma tampoco es certificable, pero proporciona las pautas para la gestión del riesgo en la seguridad de la información sobre los conceptos generales definidos en la norma ISO/IEC 27001. Esta norma está diseñada ayudar a la aplicación exitosa de la seguridad de la información basada en un enfoque de gestión de riesgo.

  Existen otras normas en ISO /IEC, pero se indicaron las que serán utilizadas para el desarrollo del trabajo de grado. [13]

1.4. ¿CÓMO SE IMPLEMENTA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)?

El modelo ISO/IEC 27001 indica que un Sistema de Gestión de la Seguridad de la Información (SGSI), debe ser formado por los siguientes documentos:

1.4.1. Alcance y límites de un SGSI.

El estándar ISO/ISC 27001, en su ítem 4.2.1 sugiere lo siguiente “Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance“.

Dicho de otra manera, es el punto de partida para establecer el SGSI, permitiendo identificar claramente las dependencias, relaciones y límites de la organización, incluyendo aquellas partes que no se tiene a considerar, dentro y fuera de la organización.

La ilustración 2, es un ejemplo capaz de definir un alcance, considerado como el método de las elipses de Alberto G. Alexander [14], permitiendo con gran precisión, poder identificar posteriormente los activos de información los cuales son el eje principal del modelo. Este método permite inicialmente distinguir los procesos y subprocesos que conforman el proceso. A cada proceso se le identifica sus respectivos procesos.

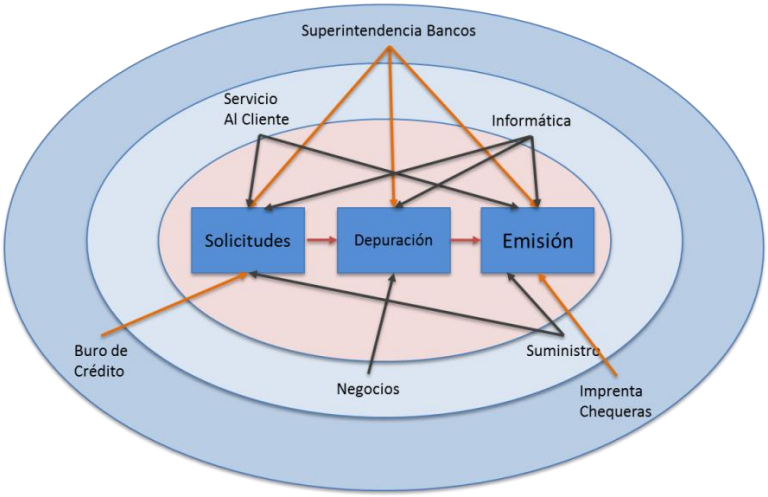

Ilustración 2: Desarrollo de la Metodología de las elipses

De la ilustración 2 se tiene, en la elipse intermedia, consiste en identificar las distintas relaciones que los procesos de la elipse concéntrica tienen con otros procesos de la organización. Y finalmente en la elipse externa, se identifican aquellas organizaciones que no hacen parte de la empresa pero tiene un tipo de interacción con los procesos y subprocesos de la elipse concéntrica. A esto le añade la dirección con que lleva la información, las cuales se representan por flechas en las respectivas elipses.

1.4.2. Política de un SGSI.

Se define como un contexto de planificación y control para establecer límites de conducta aceptable, limitar las decisiones y estándares. El objetivo de la política en un SGSI, es proporcionar apoyo por la alta gerencia de acuerdo con los requerimientos de la empresa ya que es un documento que la organización debe establecer para afirmar la implementación de la seguridad de la información en la empresa. Este documento debe ser aprobado por la alta gerencia y asegurarse que todos los miembros de la empresa la han entendido, teniendo presente que es un documento que tiene que estar completamente actualizado, por lo cual debe ser revisado y modificado anualmente. Existen tres casos en los cuales es impredecible su revisión y actualización; el primero, después de grandes incidentes de seguridad, el segundo después de una auditoria del sistema sin éxito y el tercero, frente a cambios que afectan a la estructura de la organización.

- Violación a la política de seguridad de la información y medidas disciplinarias: la violación a las políticas de seguridad de la información, es una declaración muy poderosa, debido a que

asegura que las medidas disciplinarias se pueden tomar en contra de un usuario si no se adhiere a la política. Es muy importante que esta declaración este directamente relacionada con la política general y comportamiento de la organización.

1.4.3. Análisis y Evaluación de Seguridad de la Información.

El proceso de evaluación del riesgo permite a una organización alcanzar los requerimientos establecidos por el estándar, con el fin de ayudar a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La evaluación del riesgo es el proceso de comparar los diferentes riesgos con los criterios establecidos, para determinar el grado de importancia, el objetivo de esta evaluación es identificar y evaluar los riesgos; los cuales son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad.

El riesgo se evalúa contemplando tres elementos básicos:

1. Estimando el valor de los activos de riesgo.
2. Probabilidad de ocurrencia del riesgo.
3. Valoración de los riesgos de los activos.

1.4.4. Valoración de Riesgos.

Es parte fundamental para el desarrollo y operación de un Sistema de Gestión de Seguridad de la Información (SGSI) los cuales se requiere la valoración de la criticidad de los activos, se identifican las amenazas y su probabilidad de ocurrencia además de las vulnerabilidades del área de Recaudos. La norma ISO/IEC 27001 permite determinar la metodología de gestión de riesgos que mejor se ajuste según las características del área mencionada.

La Metodología de Evaluación del Riesgo, propone un organigrama que establece los roles necesarios y como se vinculan entre sí en cada una de las etapas de implementación del SGSI. Esta metodología, se emplea para realizar la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos que estén relacionados a los activos de información, mencionados en el alcance. Este proceso es dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse de alguna manera.

Finalmente se realiza un informe de Evaluación de Riesgo; de donde su objetivo es reflejar la identificación, localización y valoración de la exposición de los riesgos. El análisis de esta información, permitirá identificar el origen de los riesgos y las medidas preventivas para eliminar o reducirlos.

Para este trabajo de grado se ha determinado que COBIT 5 es capaz de realizar la Valoración de Riesgos para el Área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca, presentada en el capítulo 2.

1.4.5. Tratamiento de Riesgo.

Plan de Tratamiento de Riesgos, es un documento que una vez se culmina la identificación, valoración, y la definición de los riesgos, se debe establecer cuáles son los controles o medidas que se van a diseñar, establecer, implementar o mejorar para cada riesgo que no haya quedado en los niveles tolerables o aceptables.

El proceso de tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

1.4.6. Declaración de Aplicabilidad.

Declaración de aplicabilidad SOA (Statement of Applicability) [15], es un documento que contiene todos los objetivos de control y los controles contemplados por el Sistema de Gestión de Seguridad de la Información (SGSI), los cuales se concluyó en los resultados de los procesos de evaluación y tratamiento del riesgo. Estos controles, son una selección del anexo A de la norma ISO/IEC 27001, además es posible incluir controles y objetivos de control que no estén enlistados en la norma.

Este documento se desarrolla después de la etapa del tratamiento de riesgos, donde se definen las acciones para mitigar, transferir o aceptar el riego existente, es en ese punto donde se precisan las medidas de seguridad que estarán plasmadas en el SOA, en el documento además se especifica si estas medidas están o no siendo aplicadas.

1.5. MARCO LEGAL Y JURÍDICO DE LA SEGURIDAD DE LA INFORMACIÓN.

Todos los días nos enfrentamos a nuevas formas de delito informático que afectan a la seguridad de la información en las empresas; hoy en día, con el desarrollo de la tecnología ha proporcionado la creación de un marco legal y jurídico que adopta a todas las partes interesadas en el uso de la tecnología, el intercambio y tratamiento de la información a través de leyes.

Por ello, cumplir con las leyes o documentos vigentes en Colombia, es un requisito para poder implantar y certificar un Sistema de Gestión de la Seguridad de la Información, donde su cumplimiento permitirá, proteger de cualquier amenaza la información.

El Documento CONPES 3072 de 2000 "Agenda de Conectividad" busca "de gobierno en línea [16] masificar el uso de las tecnologías de información y las comunicaciones y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y socializar el acceso a la información".

El Decreto 127 de 2001 [17] fue creado el Programa Presidencial para el Desarrollo de las Tecnologías de la Información y de las Comunicaciones el cual coordina la Agenda de Conectividad. Más adelante, mediante el Decreto 3107 de 2003 [18] se suprime y trasladan sus funciones al Ministerio de Comunicaciones.

En Colombia la estrategia Gobierno en línea [19], liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, promueve la construcción de un estado más eficiente, transparente y participativo, el cual permite mejorar servicios con la colaboración de la sociedad mediante el aprovechamiento de la tecnología de la información y las comunicaciones TIC. Este con el fin de mejorar la calidad de vida de los colombianos. El modelo de Seguridad de la Información para entidades del Estado, se apoya en la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en Línea – SANSI [20], el cual permite el cumplimiento de los principios definidos de la Ley 1341 de 2009 [21] y en la Estrategia de Gobierno en Línea, que corresponden a la protección de la información del individuo y la credibilidad y confianza en el Gobierno en línea.

El Sistema Administrativo de Seguridad de la Información SANSI, institución que le da la facultad al Presidente de la República de conformar la Comisión Nacional de Seguridad de la Información para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento de las políticas y controles del Modelo de Seguridad en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que pertenezcan a la cadena de prestación de servicios.

El SANSI es un sistema institucional que reúne a todos los actores públicos, privados, la academia y la sociedad civil involucrados en la seguridad nacional de la información. Así mismo, incorpora el conjunto de reglas y normas que rigen las interacciones entre estos actores.

En este sentido, el SANSI coordinará las actividades relacionadas con la formulación, ejecución, seguimiento, mantenimiento de las políticas y lineamientos necesarios para fortalecer la adecuada gestión de la seguridad de la información

nacional, y mejorar el Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea, pero esta vez no orientado hacia una organización en particular sino a todos los actores y entidades involucradas.

Ilustración 3: Sistema Administrativo Nacional de Seguridad de la información.

La Ley 1273 de 2009 modifica el Código Penal [22] y crea un nuevo bien jurídico tutelado que se denomina “protección de la información y de los datos”.

2. METODOLOGIA PARA LA VALORACION DE RIESGO: COBIT 5.

2.1. ¿QUÉ ES COBIT 5?

Es producto de la mejora estratégica de ISACA impulsando la próxima generación de guías sobre el Gobierno y la Administración de la información y los Activos Tecnológicos de las Organizaciones, construido sobre más de 15 años de aplicación práctica, ISACA desarrolló COBIT 5 para cubrir las necesidades de los interesados, y alinearse a las actuales tendencias sobre técnicas de gobierno y administración relacionadas con la TI.

COBIT 5 es una guía de mejores prácticas, dirigido al control y supervisión de tecnología de la información (TI), para el Gobierno y para la gestión de la empresa. Se trata de una ayuda a los profesionales de TI y líderes de las organizaciones para llevar a cabo sus responsabilidades en la gestión y gobierno de TI, proporcionándoles así valor al negocio.

Para que la Organización tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo, la información es un recurso clave para las empresas y desde el momento en la información se crea hasta que es destruida. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

Si bien existen varios Marcos de trabajo o referencia de Gobierno y Control Interno de TI que pueden ser aplicados en el ámbito de Tecnologías de la Información, uno de los más usados a nivel de Auditoria de Sistemas es COBIT, actualmente en su versión 5. El mismo ha sido desarrollado y propulsado por la ISACA.

2.2. COBIT 5 PARA RIESGOS.

Presenta dos perspectivas en el uso de COBIT en un contexto de riesgo: la función de riesgo y la gestión de riesgos. La perspectiva de la función de riesgo se centra en lo que se necesita para construir y mantener la función de riesgo en la empresa. La perspectiva de la gestión de riesgos se centra en los procesos básicos de gobierno y gestión del riesgo para optimizar el riesgo y en cómo identificar, analizar, responder y reportar sobre el riesgo a diario.

COBIT 5 para Riesgos, destacado en la ilustración 4, se basa en el marco COBIT 5, centrándose en el riesgo y proporcionando una orientación más detallada y

práctica a los profesionales de riesgo y otras partes interesadas en cualquier nivel de la empresa.

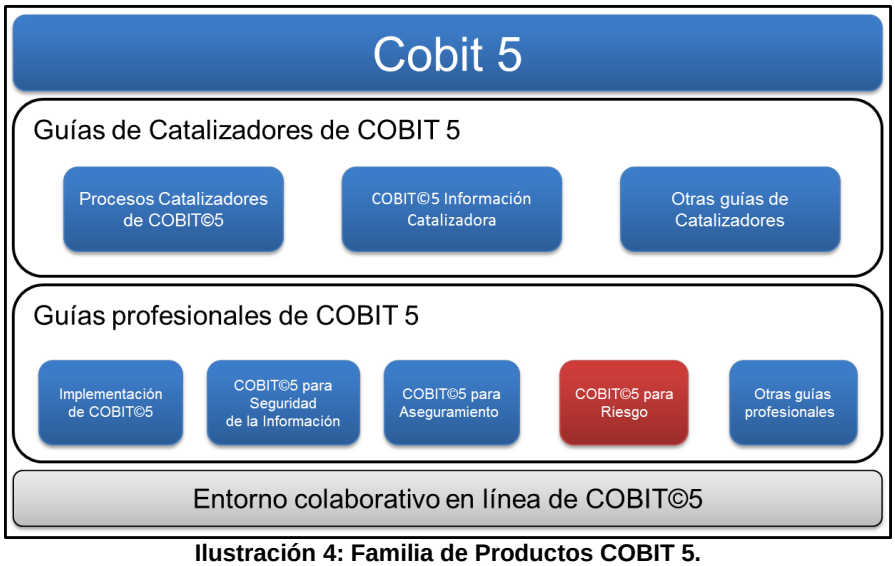

Ilustración 4: Familia de Productos COBIT 5.

Fuente: Familia de productos Cobit 5 (ISACA COBIT 5 Para riesgos, figura 1)

2.2.1. Riesgo.

Un riesgo de negocio, específicamente, el riesgo de negocio asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa. El riesgo de TI consiste de eventos relacionados a TI que potencialmente podrían impactar al negocio. El riesgo de TI puede darse con una frecuencia e impacto inciertos, generando desafíos en el logro de las metas y los objetivos estratégicos.

2.2.1.1. Los riesgos de TI pueden ser categorizados:

- **Riesgo en la habilitación de valor/beneficio de TI:** Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocio.
- **Riesgo en la entrega de programas y proyectos de TI:** Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos que forman parte de portafolios de inversión.
- **Riesgo en la entrega de operaciones y servicios de TI:** Asociado con todos los aspectos del negocio como el desempeño normal de sistemas

y servicios de TI, los que pueden destruir o reducir el valor para la empresa.

2.2.2. La perspectiva de la gestión de riesgos

Esta perspectiva comprende el gobierno y la gestión, es decir, cómo identificar, analizar y responder al riesgo, y cómo utilizar el marco COBIT 5 para dicho propósito. Esta perspectiva requiere implementar procesos principales del riesgo (EDM03 Asegurar la optimización del riesgo y APO12 Gestionar el riesgo). Estos procesos se describen en detalle en el apéndice C de COBIT 5 para Riesgos.

2.3. PRINCIPIOS DE COBIT 5

Cobit 5 se basa en cinco principios claves (ver ilustración 5), estos habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión, el uso de información y tecnología para el beneficio de las partes interesadas.

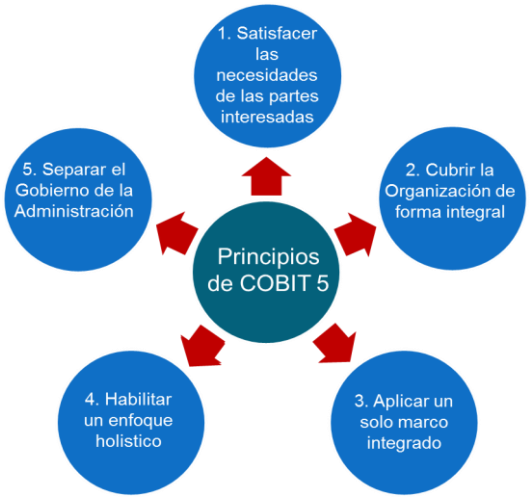

Ilustración 5: Principios de COBIT 5.

Fuente: Principios de COBIT 5 (ISACA COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, figura 2)

2.3.1. PRINCIPIO 1: Satisfacer las necesidades de las partes interesadas

Es crítico definir y vincular los objetivos empresariales y los objetivos relacionados con TI, COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI, la optimización del riesgo es uno de los tres componentes del objetivo general de la creación de valor de la empresa.

2.3.1.1. Cascada de Metas de COBIT 5

COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Se permite establecer metas específicas en todos para soportar la alineación entre las necesidades de la empresa, soluciones y servicios de TI.

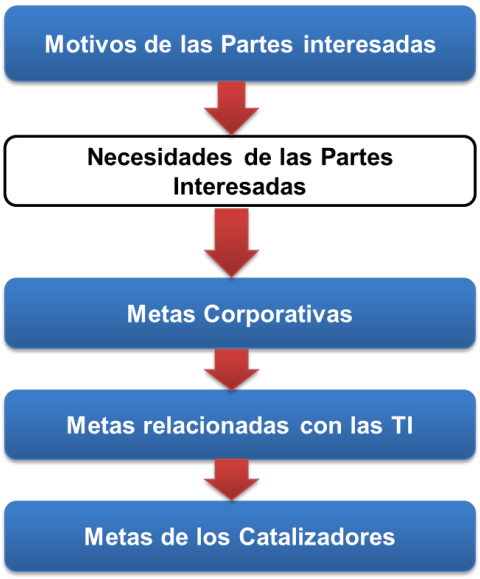

Ilustración 6: Visión General de la Cascada de Metas de COBIT 5

Fuente: Visión General de la Cascada de Metas de Cobit 5 (ISACA COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, figura 3)

La cascada de metas es importante porque permite la definición de prioridades de implementación, mejora y aseguramiento del gobierno de las TI de la empresa, que se basa en metas corporativas (estratégicas) de la empresa y el riesgo relacionado.

2.3.2. PRINCIPIO 2: Cubrir la empresa de extremo a extremo

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, cubre todas las funciones y procesos dentro de la empresa y considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos internos y externos y orienta todo hacia la gestión del riesgo.

2.3.3. PRINCIPIO 3: Aplicar un solo marco integrado

Usar un solo marco de gobierno integrado puede ayudar a las organizaciones a brindar valor óptimo de sus activos y recursos de la TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes (ver ilustración 7), y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

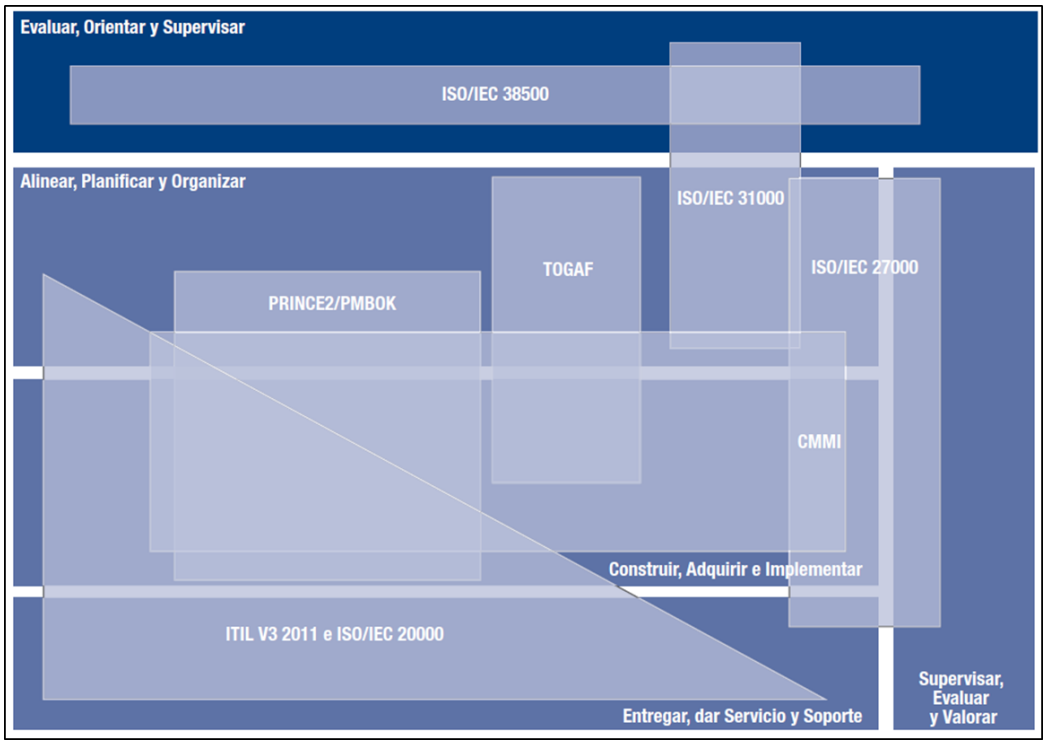

Ilustración 7: Cobertura de COBIT 5 con otros estándares y marcos de trabajo.

Fuente: Cobertura de Cobit 5 de otros estándares y marcos de trabajo (ISACA COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, figura 25)

Dentro del marco de las normas ISO existe una comparación entre la ISO/IEC 27005 y COBIT para Riesgos donde se resalta que proceso como lo define ISO/IEC 27005 está totalmente cubierto por los distintos procesos y prácticas del modelo de COBIT 5 para Riesgos, el cual proporciona una guía más amplia que no están cubiertas por ISO/IEC 27005, tales como el gobierno de los riesgos y las reacciones a eventos.

2.3.4. PRINCIPIO 4: Hacer posible un enfoque holístico

El gobierno de TI empresarial requiere de un enfoque holístico que tome en cuenta muchos componentes, también conocidos como catalizadores. Los catalizadores

se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa.

2.3.5. PRINCIPIO 5: Separar al gobierno de la Gestión

Los procesos de gobierno aseguran que los objetivos se alcancen mediante la evaluación de las necesidades de los interesados, el establecimiento de la dirección a través de la priorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento y el progreso.

2.3.5.1. Modelo de referencia de procesos de COBIT 5

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

1. Gobierno: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión. En COBIT 5 para Riesgos, el proceso EDM03 asegura la optimización del riesgo y es apoyado por los catalizadores relacionados.
2. Gestión: Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar, supervisar, y proporciona cobertura extremo a extremo de las TI, los cuatro dominios son:
    - Alinear, Planificar y Organizar.
    - Construir, Adquirir e Implementar.
    - Entregar, dar Servicio y Soporte.
    - Supervisar, Evaluar y Valorar.

En COBIT 5 para Riesgos, el proceso APO12 Gestionar el riesgo, conjuntamente con los catalizadores, permiten a la empresa construir, ejecutar y supervisar una eficiente y efectiva función de gestión de riesgos.

La ilustración 8, muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5 para riesgo se resalta los procesos clave que soportan COBIT 5 para riesgo (mostrados en rosa oscuro), así como los otros procesos de soporte (mostrados en rosa claro) y los procesos principales del riesgo (mostrados en celeste)

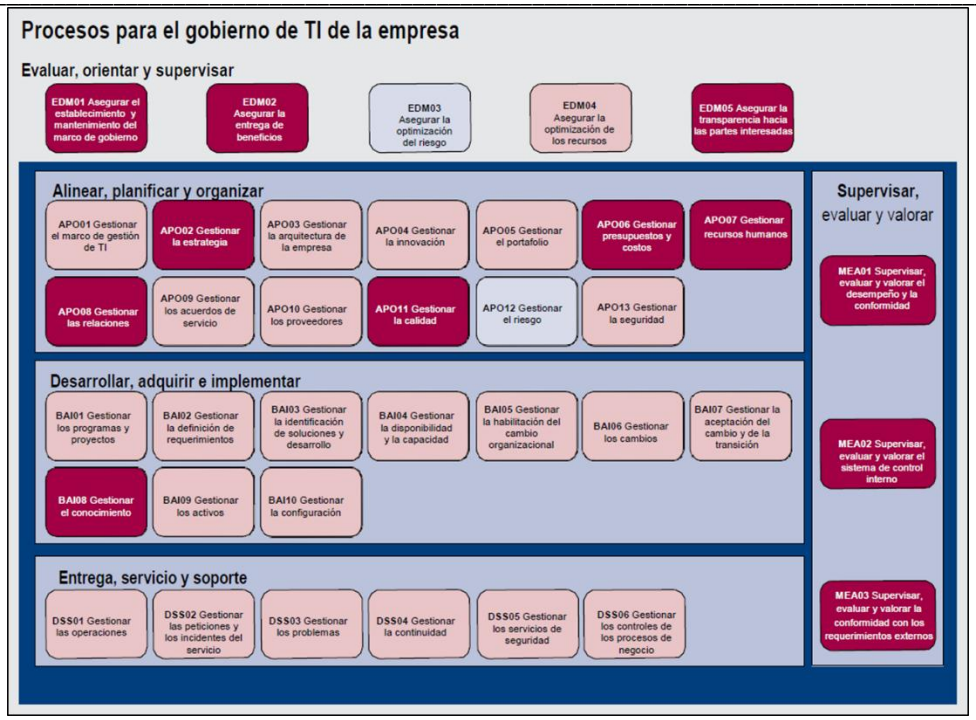

Ilustración 8: Procesos de Soporte de la Función de Riesgos.

Fuente: Procesos de Soporte de la función de riesgos (ISACA COBIT 5 Para riesgos, figura 18)

De los 37 procesos de gobierno y gestión de COBIT 5 para riesgo y según la perspectiva que identifica a los procesos EDM03 y al proceso APO12 como analizar y comprender el riesgo, el cual es nuestro objetivo para el desarrollo de este trabajo de grado.

2.4. Escenarios de Riesgo

ISACA establece el concepto de Escenario de Riesgos, como una descripción de un posible evento o suceso que, en caso de ocurrir, tendrá un impacto incierto en el logro de los objetivos de la empresa.

Un elemento de información clave que se utiliza en el proceso principal de la gestión de riesgos APO12 es el uso de escenarios de riesgo (ilustración 9).

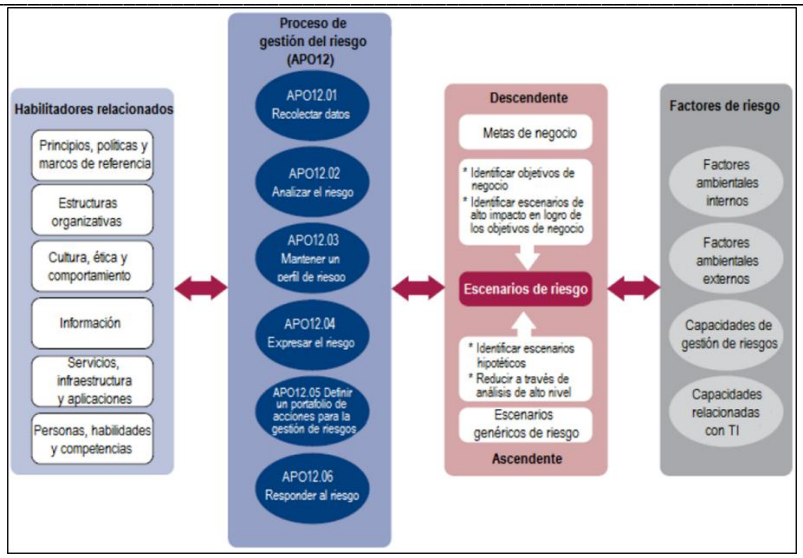

Ilustración 9: Panorama de Escenarios de Riesgo.

Fuente: Panorama de escenarios de riesgo (ISACA COBIT 5 Para riesgos, figura 34)

Un escenario de riesgo es la descripción de un posible evento que, si ocurre, tendrá un impacto incierto en el logro de los objetivos de la empresa. El impacto puede ser positivo o negativo.

La ilustración 12, también muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes:

- Un enfoque descendente, donde se comienza desde los objetivos generales de la empresa y se realiza un análisis de los escenarios de riesgo de TI más relevantes y probables que impactan a los objetivos de la empresa. Si los criterios de impacto utilizados durante el análisis de riesgos están bien alineados con los impulsores de valor real de la empresa, se desarrollarán escenarios de riesgo relevantes.
- Un enfoque ascendente, donde se utiliza una lista de escenarios genéricos para definir un conjunto de escenarios más relevantes y personalizados, aplicados a la realidad individual de la empresa.

Los enfoques son complementarios y deberían ser utilizados de forma simultánea.

Una vez definido el conjunto de escenarios de riesgo, puede ser utilizado para el análisis de riesgos, donde se evalúan la frecuencia y el impacto del escenario. Los factores de riesgo son componentes importantes de esta evaluación.

2.4.1. Flujo de trabajo en el desarrollo de escenarios de riesgo

Pasos sugeridos:

1) Utilizar la lista de ejemplos de escenarios de riesgo genéricos para definir un conjunto manejable de los escenarios de riesgo a la medida de la empresa.
2) Efectuar una validación respecto de los objetivos de negocio de la entidad.
3) Afinar los escenarios seleccionados sobre la base de la validación anterior, detallándolos a un nivel acorde con la criticidad de la entidad.
4) Reducir el número de escenarios a un conjunto manejable. “Manejable” no significa un número fijo, sino que debería estar alineado con la importancia global (tamaño) y la criticidad de la unidad.
5) Mantener todos los escenarios en una lista para que puedan ser re-evaluados en el siguiente proceso de validación y que se puedan incluir para un análisis detallado, si se vuelven relevantes en un cierto tiempo.
6) Incluir un evento no específico en los escenarios, p.ej., un incidente no cubierto en otros escenarios.

Una vez definido el conjunto de escenarios de riesgo, puede ser utilizado para el análisis de riesgos, donde se evalúan la frecuencia y el impacto del escenario. Los factores de riesgo son componentes importantes de esta evaluación.

2.4.2. Factores de riesgo

Los factores de riesgo son aquellas condiciones que influyen en la frecuencia y/o impacto en el negocio de los escenarios de riesgo. Pueden ser de diferente naturaleza y se pueden clasificar en las siguientes categorías:

La ilustración 10 muestra factores de riesgo:

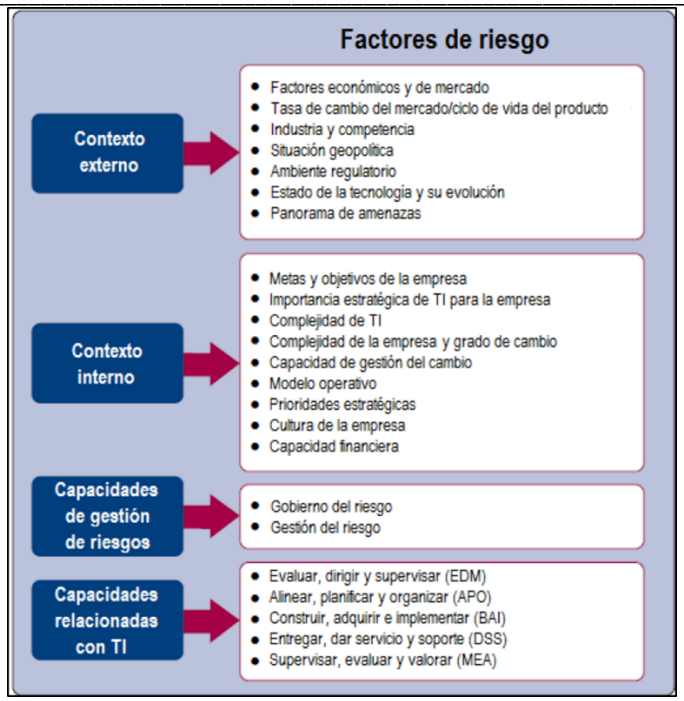

Ilustración 10: Factores de Riesgo.

Fuente: Factores de Riesgo (ISACA COBIT 5 Para riesgos, figura 35)

2.4.3. Estructura de escenarios de riesgos de TI

Un escenario de riesgo de TI es una descripción de un evento relacionado con TI que, en caso de ocurrir, puede conducir a un impacto en el negocio. Para que los escenarios de riesgo estén completos y sean utilizables para fines de un análisis de riesgos, deben contener los siguientes componentes, como se muestra en la figura 11:

- Actor: Lo que genera la amenaza que aprovecha una vulnerabilidad. Los actores pueden ser internos o externos y pueden ser humanos o no humanos:
- Tipo de amenaza (la naturaleza del evento): malicioso, accidental, falla de un proceso bien definido, fenómeno natural.
- Evento: revelación de información confidencial, la interrupción de un sistema o de un proyecto, el robo o la destrucción. También incluye el diseño inefectivo de los sistemas y procesos, el uso inadecuado, los cambios en las normas y regulaciones que impactarán materialmente sobre el sistema, la ejecución inefectiva de los procesos,

- Activo/recurso: Recurso sobre el cual actúa el escenario. Un activo es cualquier elemento de valor para la empresa que puede ser afectado por el evento y dar lugar a un impacto en el negocio
- Tiempo: Dimensión, donde lo siguiente podría ser descrito, si es relevante para el escenario:

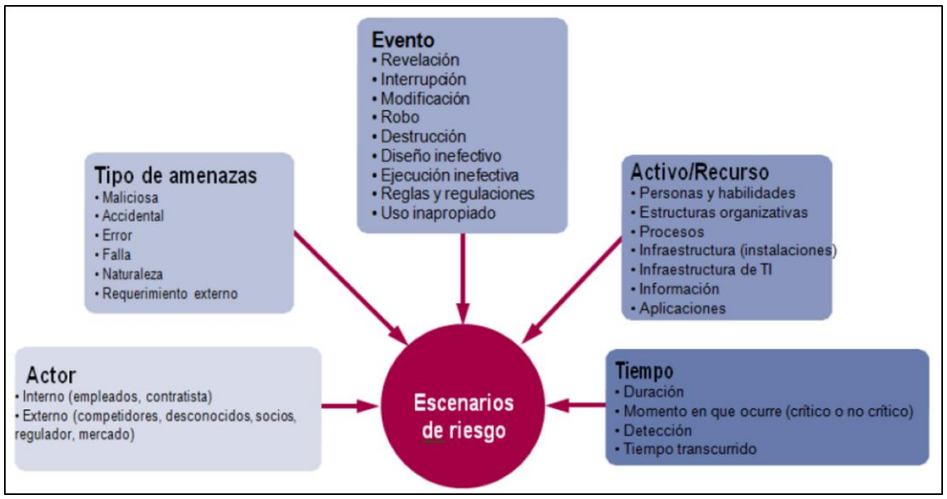

Ilustración 11: Estructura de escenarios de riesgo.

Fuente: Estructura de Escenarios de Riesgo (ISACA COBIT 5 Para riesgos, figura 36)

2.5. RESPUESTA AL RIESGO

2.5.1. Flujo y opciones de respuesta al riesgo

El propósito de definir una respuesta al riesgo es alinearla con el apetito de riesgo definido por la empresa. En otras palabras, una respuesta necesita ser definida de tal manera que todo el futuro riesgo residual posible resulte dentro de los límites de tolerancia definidos.

Esta evaluación de respuesta al riesgo no es un esfuerzo de una sola vez, sino que es parte del ciclo del proceso de gestión de riesgos. Cuando el análisis de riesgos de todos los escenarios de riesgo identificados, después de comparar el riesgo contra el retorno potencial, muestra que el riesgo no está alineado con el apetito de riesgo o los niveles de tolerancia definidos, se requiere una respuesta. Esta puede ser cualquiera de las cuatro posibles respuestas explicadas a continuación:

2.5.1.1. Evitar el riesgo.

Significa dejar de hacer las actividades o salir de las condiciones que permiten que el riesgo se presente. Evitar el riesgo sólo aplica cuando ninguna otra respuesta al riesgo es adecuada. Este es el caso cuando:

- No existe ninguna otra respuesta efectiva en costo que pueda ser exitosa para disminuir la frecuencia o el impacto debajo de los umbrales definidos para el apetito de riesgo.
- El riesgo no puede ser compartido o transferido.
- El nivel de exposición ha sido considerado inaceptable por la gerencia.

2.5.1.2. Aceptar el riesgo.

Aceptar significa que se reconoce la exposición a la pérdida pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada. Aceptar un riesgo supone que se conoce el riesgo y que la gerencia ha tomado una decisión informada para aceptarlo como tal.

2.5.1.3. Compartir/Transferir el riesgo.

Compartir significa reducir la frecuencia o el impacto del riesgo transfiriendo o compartiendo una porción del riesgo.

2.5.1.4. Mitigar el riesgo.

Significa tomar acciones de mitigación para reducir la frecuencia y/o el impacto de un riesgo.

COBTI 5 para Riegos presenta una guía elaborada de los escenarios de riesgos genéricos, que expresan las situaciones más importantes que pueden afectar a la organización con respecto al uso de las tecnologías y que se puede utilizar aunque se advierte que el análisis no se debe basar únicamente en esta, se menciona la capacidad de generar escenarios de riesgo propios acorde a la institución y sus necesidades.

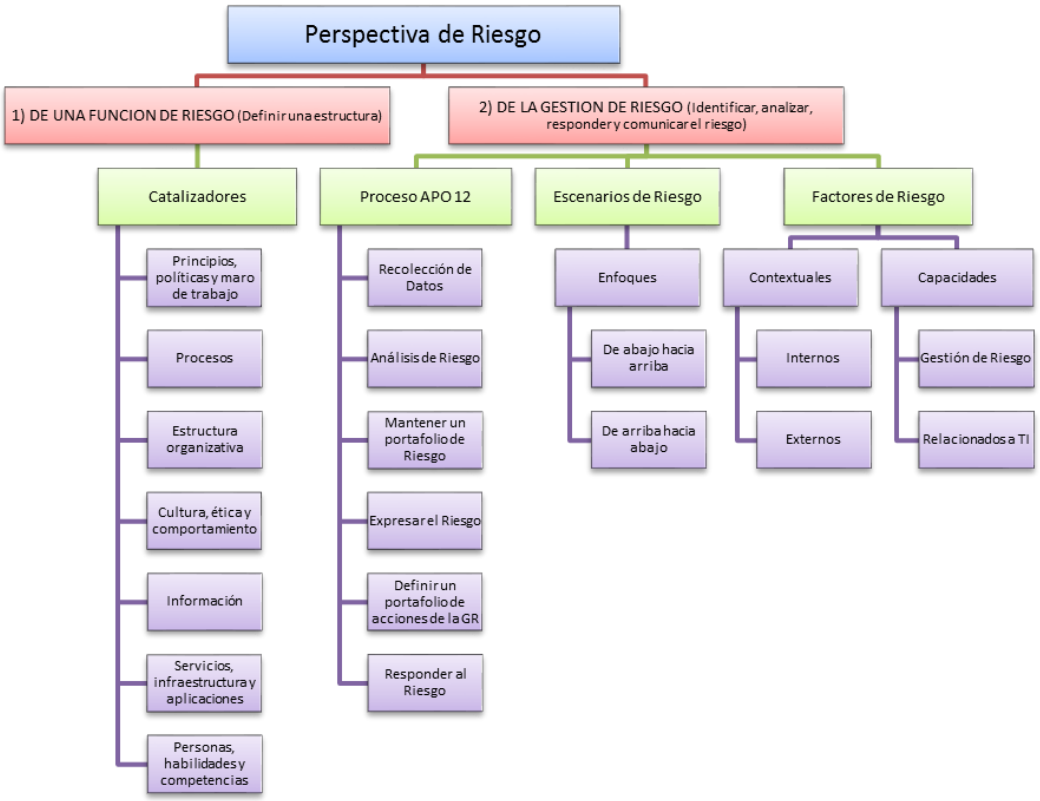

Ilustración 12: Perspectiva de riesgo.

Para una mayor comprensión acerca de cómo COBIT 5 para riesgos, la ilustración 12, complementa con los diferentes estándares internacionales se presenta a continuación un esquema donde se puede apreciar que el MARCO COBIT 5 para riesgos abarca de manera indirecta los estándares anteriormente analizados, pero aun así este requerirá alinearse ya sea con uno o con los dos conjuntamente dependiendo de las necesidades de cada entidad para lograr una gestión óptima de los riesgos.

3. ESTUDIO DE CASO.

Para el desarrollo del trabajo de grado, es necesario utilizar el método estudio de caso, el cual es propuesto en (Using a protocol template for case study planning, Brereton), con el fin de analizar y profundizar el contexto de la problemática por la que pasa la organización; este modelo especifica las fases para poder desarrollar adecuadamente un caso de estudio. Como también se tendrá en cuenta el artículo de investigación "A research frameword for building SPI proposal in small organizations: The Competisoft experiencie" de los autores Francisco Pino, Felix Garcia, Mario Piattini y Hanna Oktaba [23], dicho artículo combina tanto estudio de caso e investigación-acción, lo cual es precisamente el enfoque que se le da a este trabajo de grado, permitiendo así poder llevar a cabo la adaptación de la metodología COBIT 5 para Riesgos basado en las experiencias y prácticas.

El estudio de caso permite conocer a fondo el problema o algún hecho de inconformidad que se encuentra la organización, es por esto, que se decide usar el estudio de caso como estrategia que permita conocer la problemática de la organización a gran profundidad, obtener respuestas de ciertas cuestiones para la adaptación de la metodología y por consiguiente recolectar toda la información que sea necesaria.

Dentro de este marco se hace necesaria la siguiente pregunta, ¿Es la metodología COBIT 5 adecuada para la valoración del riesgo en la fase de planeación de un SGSI bajo la norma ISO 27001 en la División Financiera de la Universidad del Cauca? Con el objetivo de encontrar respuesta a dicha pregunta se siguen los siguientes ítems:

3.1. DISEÑO

El tipo de diseño para el desarrollo de este trabajo de grado corresponde al Simple / Holístico, el primero debido a que es una sola unidad organizacional, más específicamente el área de Recaudos de la división de Gestión Financiera de la Universidad del Cauca y el segundo porque tiene una única unidad de análisis, la cual hace referencia al Sistema de Gestión de Seguridad de la Información SGSI.

3.1.1. OBJETO DE ESTUDIO

La Universidad del Cauca cuenta actualmente con sistemas que generan y manejan información crítica, lo cual hace necesaria la utilización de normas que ayuden al manejo de la información, con el propósito de tener un control integral y uniforme de ella.

Es así que se tiene la necesidad de la implantación de un Sistema de Gestión de Seguridad de la Información SGSI, el cual tenga como objetivo de estudio la integración de las normas ISO / IEC 27000 y COBIT 5 para Riesgos, lo cual permite la realización de la valoración de los riesgos encontrados en el área de Recaudos de la división de Gestión Financiera de la Universidad del Cauca.

3.1.2. METRICAS

En todo sistema surgen controversias entre quien recoge los datos, quien los aporta y quien los analiza, de ahí la importancia de poder reproducir resultados; por este motivo, es esencial que el modelo de métricas nazca en el mismo instante en que nace el SGSI puesto que todo el mundo que participa en él será consciente que lleva el máximo apoyo de la gerencia y por lo tanto deberá siempre tomar una actitud participativa y positiva, esto lleva a decir que el sistema que se propuso fue aceptado por los entes encargados del área de recaudos quienes junto con el jefe de la división revisaron y aprobaron los resultados obtenidos.

3.1.3. SUJETOS DE INVESTIGACION

Los sujetos o participantes autorizados e involucrados en la prestación de la información requerida para el desarrollo de este trabajo son los siguientes:

- En la división de Gestión Financiera se contó con el jefe encargado de la división y el técnico administrativo, el cual reconoce, revela, controla y garantiza el recaudo y registro de los recursos financieros a los cuales la Universidad tiene derecho, fijan las tarifas de cobro a facturar en SIMCA y SQUID y termina con el archivo de los documentos.
- En la división de las TIC se contó con el ingeniero encargado de los servidores de la universidad, el cual es el responsable de la operación y mantenimiento de los servidores requeridos por el área de recaudos de la división de gestión financiera.

3.1.4. INVESTIGADORES

Los investigadores o participantes del desarrollo de este trabajo de grado son los siguientes:

Milena Natalia Cruces Cerón. Estudiante de último semestre de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, 2016.

Juan Pablo Mora Palacios. Estudiante de último semestre Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, 2016.

3.1.5. SELECCIÓN DEL CASO

Teniendo presente el impacto que se tiene hoy en día con el riesgo de la información, la Universidad del Cauca por medio del Rector Delegatorio, soportado por la resolución numero R 005 de 2015 (7 de Enero) (anexo A), autoriza la realización del proyecto "Implantación y Certificación del Sistema de Gestión de la Seguridad de la Información SGSI de la Universidad del Cauca" De donde la resolución dice: "Es necesario proteger los activos de información y para tal efecto es indispensable la implementación de un (SGSI)". Es por eso que da a conocer la necesidad de implantar un SGSI para el área de Recaudos con el fin de que se brinde protección de los activos de información con los cuales cuenta dicha área, debido a que es una de las más importantes, puesto que es la encargada del manejo de toda la información correspondiente a los ingresos presupuestables de la Universidad del Cauca; así lo constata el análisis del método de las elipses llevado a cabo por los integrantes del procedimiento y es detallado en el capítulo 5, sección 5.2.1.3.

3.1.6. PROCEDIMIENTO DE CAMPO

El procedimiento de campo se identifica en la ilustración 13 la cual hace una breve descripción de cada una de las fases 5, 6,7 y 8 de la ISO/IEC 27003 para la implantación de un SGSI al área de Recaudos de la división de gestión Financiera.

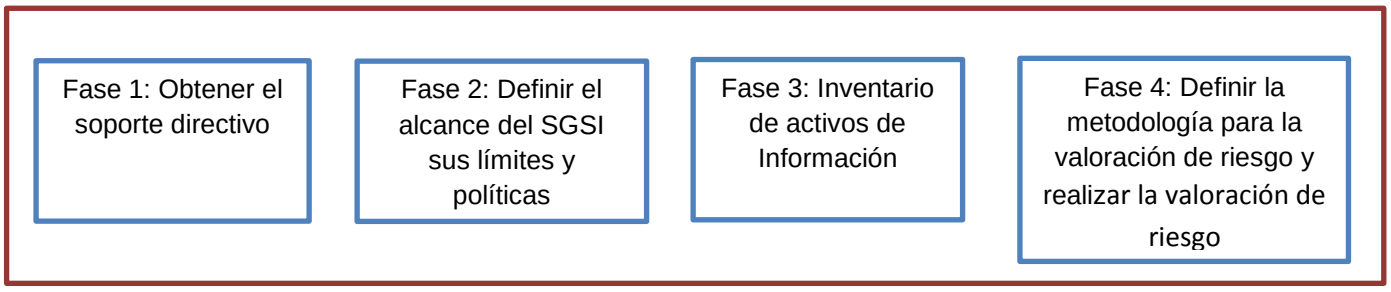

Ilustración 13: Fases de la ISO/IEC 27003

En la fase 1 se obtuvo todo el soporte y autorización pertinente para la captación de la información requerida para la implementación del SGSI por parte del ente encargado de recaudos; a continuación en la fase 2 se definió el alcance, límites y las políticas del SGSI del recaudos; posteriormente en la fase 3, se identificaron los activos de información con su respectiva clasificación en la que se encuentran; y finalmente en la fase 4, se definió la metodología para la valoración de riesgos para de esta manera realizar la respectiva valoración de riesgos a los activos de información, esta realización se determinó con el modelo adaptado que se

desarrolló con las ISO/IEC 27000 y COBIT 5 para riesgos, la cual esta analizada y descrita en el capítulo 4.

Cabe mencionar que todo el respetivo desarrollo detallado y minucioso de cada una de estas fases, se encuentra en el capítulo 5 específicamente en los ítems 5.1, 5.2, 5.3 y 5.4.

3.1.7. INTERVENCIÓN

Para el desarrollo de este trabajo, se tuvo en cuenta la resolución estipulada por el rector delegatorio el cual da a conocer la necesidad de la implementación de un Sistema de Gestión de Seguridad de la Información SGSI; seguidamente se realizó la reunión con el jefe encargado de la vicerrectoría administrativa informándole a cerca del trabajo que se desea desarrollar, de esta manera se generó una autorización al jefe de la división de gestión financiera para permitir la ejecución del proyecto; dentro de este marco, el jefe autoriza al técnico administrativo encargado del área de Recaudos para la recopilación de la información necesaria por los investigadores. Así mismo se autorizó al ingeniero encargado de los servidores que prestan el servicio a recaudos, encontrado en la división de las TIC.

Es de resaltar que toda la recopilación de información para este estudio de caso se determinó mediante entrevistas individuales al personal encargado, así como también por medio de documentación y encuestas las cuales fueron aceptadas mediante actas levantadas y firmadas por cada uno de los miembros con los que se realizó.

Como resultado a todo este procedimiento se desarrolló toda la fase plan de un Sistema de Gestión de Seguridad de Información bajo la norma ISO/IEC 27001 siguiendo como guía de implementación la ISO/IEC 27003 tomando como metodología de valoración de riesgos a COBIT 5. Todo este proceso se ve reflejado en los capítulo 4 y 5 los cuales especifican cada una de las fases y etapas por las que se debe pasar para la implementación del SGSI y por último la selección de los controles y los objetivos de control de seguridad estipulados por la ISO/IEC 27002.

3.2. ANÁLISIS DEL CASO

Utilizar COBIT 5 y las normas ISO/IEC 27000 han sido de vital importancia debido a que permitió la implementación del sistema de gestión de seguridad de la información SGSI, lo cual fue realizado bajo la revisión y supervisión del desarrollo del trabajo del personal encargado de la división, como también del director de

trabajo de grado; esto permite concluir que si es viable la implementación de COBIT 5 como metodología para la valoración de riesgos en la fase plan de un Sistema de Gestión de Seguridad de la Información puesto que cumple con todos los requisitos establecidos por la norma ISO/IEC 27001.

4. MODELO DE ADAPTACIÓN

Para el desarrollo del análisis de riesgo de la fase plan de un SGSI, se propone la adaptación de una metodología utilizando COBIT 5 para Riesgos, la cual se basa en el marco COBIT 5, siguiendo correctamente en conformidad con la ISO/IEC 27005, centrándose en el riesgo y proporcionando una orientación más detallada y práctica, al mismo tiempo que cumple lo que la Norma ISO/IEC 27001 exige para lograr la certificación.

4.1. JUSTIFICACIÓN DE LA ADAPTACIÓN

Luego de un análisis del Marco Cobit 5 para Riesgos el cual puede ser aplicado a todo tipo de organización y teniendo como su fin principal alcanzar los objetivos de la entidad a través de su cascada de metas y la aplicación de siete catalizadores, este marco no es una camisa de fuerza por lo que no constituye un modelo obligatorio, al contrario busca que cada entidad estructure su Tecnología de Información tomando como base Cobit 5. Se hace necesaria la adaptación a una metodología de análisis de riesgos llevando como guía Cobit 5 para Riesgos adecuándose a la fase plan del SGSI propuesto, que sigue la normatividad ISO/IEC 27003:2010.

El siguiente modelo es propuesto con base a Cobit 5 y toda la familia de productos relacionados a TI elaborados por ISACA, serviría para la valoración y tratamiento del riesgo.

4.2 DESCRIPCION DEL MODELO ADAPTADO

Para la adaptación de esta metodología se considera el proceso APO12 que hace referencia al planteamiento, ejecución, control y evaluación de las actividades que permiten el tratamiento del riesgo lo cual corresponde al cumplimiento de la norma ISO/IEC 27003.

APO12 (Gestionar el riesgo): *Permite identificar, evaluar y reducir los riesgos relacionados a las TI de forma continua, dentro de los niveles de tolerancia establecidos teniendo en cuenta los requerimientos de la dirección.*

4.2.1. ADAPTACION A LA FASE PLAN

Fase de Plan. "*La norma da las pautas para determinar el alcance del modelo de la empresa, identificar los activos de información y tasarlos, luego hacer el análisis y la evaluación del riesgo y determinar qué activos de información están sujetos a riesgo. Seguidamente en esta fase se deben determinar las opciones para el*

tratamiento del riesgo". Fase de Ejecución. "*En la segunda fase del ciclo Deming, la llamada Implementación del SGSI, se debe elaborar el plan de tratamiento de riesgos, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas*".

Ya que Cobit 5 para riesgos no proporciona una metodología concreta de análisis de riesgo, sino que describe a través del Proceso APO12 el desarrollo recomendado de análisis que debe hacerse utilizando el enfoque de riesgos que este Marco proporciona, para ello se hizo un análisis de las recomendaciones de cada Práctica del Proceso APO12 para incluir los elementos que debe de tener una metodología de análisis de Riesgo, a continuación se muestra la adaptación completa que se hizo siguiendo la buenas prácticas de Cobit 5 para Riesgos, al Proceso APO12.

- ✓ **Catalizadores**

Para esta adaptación, tenemos la definición de siete catalizadores que apoyan la implementación de un sistema integral de gobierno y gestión de TI en la empresa utilizando Cobit 5, los cuales son factores que influyen, individual y colectivamente para el éxito del gobierno y la gestión de TI, de este conjunto de catalizadores explicados anteriormente solo se tomará uno de ellos, el de Procesos, porque este contiene el Proceso APO12 de los 37 que Cobit 5 nos proporciona y es este el que gestiona el Riesgo, ya que no es el objetivo de nuestro trabajo el implementar el Marco completo y no se ve afectado el proceso a implementar por la eliminación de estos.

- ✓ **Procesos**

Para la Adaptación de los procesos, de los 37 que la norma expone y en particular centrándonos en los dos principales (EDM03 y APO12) [26] de gestión de riesgos, eliminaremos el aporte que pretende el domino EDM (Evaluar, Orientar y Sustentar) porque está centrado únicamente al gobierno, nuestro análisis se enfocará en establecer una metodología de gestión de riesgo, por esta razón se tomará en cuenta los cuatro dominios restantes que se alinean a la gestión, pero de manera especial al proceso APO12 el cual responde al cumplimiento de los objetivos de la tesis.

A continuación se detallarán las etapas Adaptadas de cada una de las prácticas del proceso que llamaremos Fases.

- ✓ **Proceso APO 12: PROCESO DE GESTIONAR EL RIESGO.**

Las fases para el análisis de riesgo son identificadas en la ilustración 14 de acuerdo al proceso APO12 y serán detalladas a continuación:

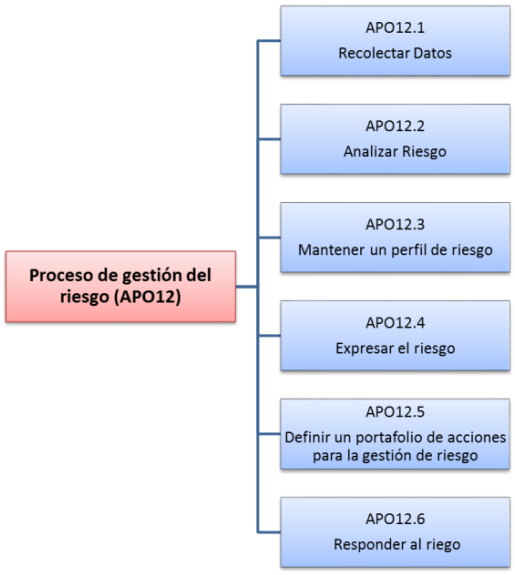

Ilustración 14: Proceso de Gestión de Riesgo.

I. Recolectar datos

La información y el conocimiento constituyen la base para la realización de la gestión de riesgos, pues el conocimiento que se obtenga de esta actividad será de vital importancia a la hora de administrar el riesgo.

Es necesario definir un método a fin de recopilar los datos existentes para su posterior análisis y clasificación, registrar datos importantes sobre el entorno actual y pasado de la entidad registrar eventos de riesgo que puedan causar impactos que desencadenen incidentes, problemas etc.

-Actualidad: Se buscara información clave, que influye en la entidad y manejo del riesgo, tanto aspectos internos como externos comprendidos en: políticas, normas, procesos, etc.

-Registro: se busca recopilar los datos y destacar los factores determinantes, en centrar las condiciones específicas de riesgo y como éstas pueden haber desencadenado problemas de riesgo

-identificar**:** se busca los múltiples eventos y factores de riesgos más recurrentes sean internos o externos para su posterior análisis y comprensión, para identificar los problemas que puedan desencadenar.

-Identificación de Procesos: Desarrollando la cascada de metas, se debe de adaptar los objetivos corporativos a las metas corporativas genéricas dadas por Cobit 5, mapeando cada una de ellas, para ser empatados con las metas genéricas de TI, para luego obtener las actividades que ayudan a identificar los riesgos mediante los escenarios de riesgos, las cuales al mismo tiempo evitaran que estos ocurran.

II. Analizar el Riesgo

La creación de valor significa la obtención de benefician a un costo óptimo de recursos mientras se optimiza el riesgo, COBIT 5 ayuda a las empresas a crear ese valor a partir de las TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y del uso de recursos, la entidad debe reconocer y conocer cuáles son los riesgos a los cuales se enfrenta, para poder prevenirlos de una forma segura mediante un plan de estrategias bien planteadas con el fin de evitar daños que repercutan en perdidas y su mal funcionamiento.

El riesgo es definido generalmente como una combinación de la probabilidad de un evento y sus consecuencias, se mide a través de la probabilidad de que una amenaza se materialice explotando en una vulnerabilidad ocasionando así un impacto.

Mediante la construcción de escenarios de riesgo conforme a los requerimientos de la entidad y teniendo en cuenta la información obtenida en la fase I, se debe de tener una calificación cualitativa y cuantitativa del nivel de riesgo, por lo que la adecuada administración de riesgos nos permite una respuesta rápida de manera que las actividades puedan ya sea recuperarse o seguir su funcionamiento normalmente.

Los conceptos para una buena calificación y un análisis que concuerde con la realidad son los siguientes:

- Frecuencia: Número de veces que se repite un evento que afecta a la entidad durante un periodo o espacio determinado.
- Magnitud**:** Es la medida con la cual determinamos las consecuencias de un evento en particular que se genera en la organización, dándonos un vistazo a la importancia que se debe de tener en dicho evento, ya sea algo negativo o positivo.

El riesgo en función de estas dos variables, el cual se puede expresar como el producto de ambos términos, dado los indicadores tomados se expresa en forma cualitativa y cuantitativa de la siguiente forma (ver ilustración 15):

Ilustración 15: Función de riesgo.

Como resultado tenemos la probabilidad y el impacto, respectivamente. Los resultados cuantitativos obtenidos sobre el nivel de riesgo se traducen en una matriz conocida como matriz de riesgo.

Para el desarrollo del presente trabajo se han definiendo tres pasos para determinar los diferentes escenarios de riesgos, siguiendo el flujo de escenarios de riesgo que Cobit 5 presenta:

a) Escenarios de Riesgo: Se trabajan con la lista de escenarios de riesgos que se presenta en COBIT 5, y además se generan nuevos escenarios que se contemplen luego de la recolección de información y tasación de activos.
b) Escenarios Importantes: Definidos los riesgos que afectan directamente a la consecución de objetivos se debe de priorizar los más riesgosos.
c) Detalle de los riesgos: Mostrar información suficientemente clara que dé una respuesta al riesgo actual que sufre la entidad.

Matriz de Riesgo:

La Matriz de Riesgos es una herramienta de gestión que permite determinar objetivamente cuáles son los riesgos relevantes para la seguridad que enfrenta una organización, pretende exponer una visualización aproximada y a la vez global de aquellos riesgos identificados que impactan a una entidad, permitiendo detectar y evaluar a simple vista si la gestión que se ha venido desarrollando ha sido efectiva.

Una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

La matriz debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de una entidad.

Esta matriz utiliza un grafo de riesgo, el cual se encuentra relacionado con la ilustración 14, mencionada anteriormente.

La valorización consiste en asignar a los riesgos calificaciones dentro de un rango, dependiendo del criterio de la persona que se encargue de su elaboración así como los calificativos empleados para la descripción del estado del riesgo.

III. Mantener un Perfil de Riesgo

Se encuentra apoyado en el proceso EDM03: Asegurar la optimización del Riesgo, que permite la definición y comunicación de la tolerancia y apetito al riesgo que mantiene la entidad para sus actividades.

- Tolerancia al Riesgo: es el nivel aceptable de fluctuación del apetito de riesgo que inicialmente ha sido definido para el logro de los objetivos de la entidad.
- Apetito al Riesgo**:** es el riesgo que ha sido definido por los administrativos de la entidad como normal dentro de las operaciones de la misma, es decir, cuánto riesgo están dispuestos a aceptar como un medio para lograr los objetivos.

IV. Expresar el Riesgo

Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada que comunica los riesgos evaluados relacionados con los activos de las organización, de esta forma se puede dar una respuesta eficiente para el tratamiento del riesgo.

La información del riesgo debe ser comunicada teniendo en cuenta los reportes siguientes:

- Plan de Comunicación de Riesgo, en el cual se bebe tener información de:
    1. Frecuencia de riesgo
    2. Tipos de riesgo
    3. Receptores de riesgo.

Este ayuda a tomar de decisiones que posibiliten la adecuada respuesta a los riesgos más probables que requieren su atención inmediata. (ISACA, 2013)

V. Definir un portafolio de acciones para la Gestión de Riesgos

Para definir las propuestas que deben hacer frente a los riesgos, se debe considerar el nivel de riesgo y las actividades clasificadas según los criterios de Cobit 5 para riesgos:

- Responsables.
- Métricas de cada actividad
- Riesgo residual

- Apetito de riesgo
- Tolerancia al riesgo
- Umbrales de tolerancia al riesgo.

Entre otros ítems relevantes que se consideren necesarios según la entidad y los requerimientos de esta, siempre dando prioridad a los riesgos que generen mayor impacto que conlleven a una perdida drástica que afecte de manera negativa la entidad.

Con los resultados obtenidos se deberá realizar una serie de análisis que brinden una mayor claridad y compresión del estado actual del riesgo, para que se pueda identificar los riesgos y sus niveles.

Para la creación de un portafolio completo de acciones para la gestión del riesgo se debe formular y aplicar la métricas o indicadores en cada actividad, y debe hacerse una evaluación periódicamente para identificar la efectividad de los controles, de esta forma se pueden hacer cambios necesarios que mejoren dicho control.

VI. Responder al Riesgo

Después de un análisis minucioso y conforme de riesgo, obteniendo los niveles de apetito de riesgo así como su tolerancia, y planeadas las actividades de acuerdo a su magnitud, la respuesta debe ser establecida a través de los planes.

Las respuestas al riesgo son las siguientes:

1. Evitar riesgo.
2. Compartir/ transferir el riesgo.
3. Aceptar el riesgo.
4. Mitigar el riesgo.

Adaptación detallada de las Fases explicadas anteriormente del Proceso APO12 con sus Prácticas y Actividades, se calibro y adapto cada una de ellas en lineamiento con la norma propuesta y la fase plan del SGSI como se ve en la tabla 1:

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
Fase 1. Recopilar datos	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con los riesgos de TI, con capacidad para varios tipos de eventos, múltiples categorías de riesgos de TI y de múltiples factores de riesgo.	No se altera		Se establece el método a seguir.
	Registrar los datos pertinentes acerca del entorno corporativo interno y externo que puedan desempeñar un papel importante en la gestión de riesgos de TI.	No se altera		Se establece el método a seguir.
	Estudiar y analizar los datos históricos de riesgos TI y la experiencia de pérdidas obtenida de datos y tendencias externos que estén disponibles, colegas del sector a través de registros de eventos basados en el sector, bases de datos y acuerdos del sector para la divulgación de eventos comunes	Se omite.		La entidad donde se está realizando la valoración no tiene información de frecuencia ni magnitud, ni tampoco escenarios de riesgo, ya que no tiene ningún servicio implantado.
	Registrar datos sobre eventos de riesgo que hayan causado o puedan causar impactos a los catalizadores del beneficio/valor de TI, a la entrega de programas y proyectos de TI, y / o a las operaciones y a la prestación de servicios de TI. Capturar la información relevante de los asuntos relacionados, incidentes, problemas e investigaciones.	Se omite.		La entidad donde se está realizando la valoración no tiene ningún tipo información de registro.
Fase 2. Analizar el riesgo	Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgos teniendo en cuenta todos los factores de riesgo y la criticidad de los activos de negocio. Establecer el alcance del análisis de riesgos después de realizar un análisis de coste / beneficio	Se altera		No se establecerá el alcance del análisis de riesgos después de realizar un análisis de coste / beneficio, ya que los procesos no serán implementados este plan, sin embargo se priorizan los más necesarios según la entidad lo requiera.

	Construir y actualizar periódicamente los escenarios de riesgo de TI, incluidos los escenarios compuestos de cascada y / o los tipos de amenazas coincidentes, y desarrollar expectativas para las actividades de control específicas, para las capacidades de detección y para otras medidas de respuesta.	Se altera.	Construir los escenarios de riesgo de TI, incluidos los escenarios compuestos de cascada utilizando las plantilla de Cobit 5 y el análisis de riesgo en la entidad	Se construirán nuevos escenarios solo negativos de acuerdo al caso y se utilizaran los genéricos de la plantilla para calibrar y ajustarse a la información obtenida. No se actualiza nada debido a que no hay ningún tipo de escenarios creados en la división.
	Estimar la frecuencia y la magnitud de la pérdida o ganancia asociada con los escenarios de riesgo de TI. Considerar todos los factores de riesgo aplicables, evaluar los controles operativos conocidos y estimar los niveles de riesgo residual	Se altera.	Estimar la frecuencia y la magnitud de la pérdida o ganancia asociada de los escenarios de riesgo de TI, a través de la probabilidad de impacto, utilizando un método mixto que combine datos cuantitativos con cualitativos, así como el uso de una matriz de riesgos para analizar los resultados	Se especifica la manera en que se medirá el impacto y de esta forma el riesgo de cada uno de los escenarios, obtenido al final los más importantes
	Comparar el riesgo residual con la tolerancia al riesgo aceptable e identificar las exposiciones que pueden requerir una respuesta al riesgo.	se omite		El riesgo residual se lleva acabo después de aplicar los controles en la fase 5 del proceso.
Fase 3. Mantener un perfil del riesgo		Se Omite		Esta Fase se encuentra basada en el proceso EDM03 cuyo aporte para nuestro análisis no es relevante, está centrado únicamente a la parte de gobierno. Por lo que nuestro análisis se enfocará en establecer una metodología de gestión de riesgo, por esta razón se tomara en cuenta los cuatro dominios restantes que se enfocan en la gestión,
Fase 4. Expresar el riesgo	Reportar los resultados de análisis de riesgos a todas las partes interesadas afectadas en los términos y formatos útiles para respaldar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y los rangos de pérdida o ganancia, junto con los niveles de confianza que permiten a la dirección equilibrar el ratio retorno-riesgo	Se altera	Reportar los resultados de análisis de riesgos a todas las partes interesadas afectadas en los términos y formatos útiles para respaldar las decisiones de la entidad. incluyendo el actor, tipo de amenaza, evento, activo o recurso	Se deben identificar claramente los riesgos de seguridad de la información y sus dueños como lo dicta la norma (NTC-ISO/IEC 27001,6.1.2 c)

	Ayudar a los tomadores de decisiones a comprender los peores casos y los escenarios más probables, las exposiciones de debida diligencia y la reputación significativa, consideraciones legales o reglamentarias.	Se omite		La fase plan del SGSI al completarse dará como resultado una evaluación de riesgo y su tratamiento de riesgo
	Reportar el perfil actual de riesgos a todas las partes interesadas, incluida la eficacia del proceso de gestión de riesgos, el control de la eficacia, las lagunas, incoherencias, redundancias, estado de remediación, y sus impactos sobre el perfil de riesgo.	Se omite		Con la actividad anterior se reporta los resultados, no se evaluara el proceso ya que no se encuentra implementado.
	Revisar los resultados de las evaluaciones objetivas de terceros, de la auditoría interna y de las revisiones de controles de calidad y asignarlos al perfil de riesgo. Revisar las lagunas identificadas y las exposiciones para determinar la necesidad de un análisis de riesgo adicional.	Se omite		La entidad donde se está realizando la valoración no tiene ningún tipo de evaluación ni controles, ni auditorias, no se planea análisis adicionales
	De forma periódica, para zonas con riesgo relativo y capacidad de riesgo paritarias, identificar oportunidades relacionadas con TI que permitan la aceptación de un mayor riesgo y mayor crecimiento y rentabilidad.	Se omite		Esta actividad le compete a los directivos de la entidad, de acuerdo al análisis de riesgos se pueda aceptar un mayor riesgo y coordinar actividades que den al negocio un valor mayor.
Fase 5. Definir un portafolio de acciones para la gestión de riesgos	Mantener un inventario de las actividades de control implantadas para gestionar el riesgo y que permita que los riesgos se adecúen al apetito de riesgo y a la tolerancia. Clasificar las actividades de control y asignarlas a las declaraciones de riesgo de TI específicas y a las agregaciones de riesgos de TI.	Se altera	Mantener un inventario de las actividades de control implantadas para gestionar el riesgo y que permita que los riesgos se adecúen al apetito de riesgo y a la tolerancia, Aplicar las prácticas y controles para la mitigación de riesgos de seguridad.	Esta actividad está directamente relacionada con el plan por lo que el nivel de riesgo debe reducirse mediante controles, de acuerdo al Numeral 6.1.2 de la norma ISO/IEC 27001:2013 Numeral 8.3 de la GTC ISO/IEC 27003:2012
	Determinar si cada entidad organizativa monitorea el riesgo y acepta la responsabilidad de operar dentro de sus niveles de tolerancia tanto individual como de portafolio.	Se omite		En la actividad anterior está completamente relacionada con lo que busca esta fase, que es la inmediata aplicación de los controles de acuerdo a la fase plan del SGSI propuesto.

	Definir un conjunto equilibrado de propuestas de proyectos destinados a reducir el riesgo y / o proyectos que faciliten las oportunidades empresariales estratégicas, teniendo en cuenta el coste / beneficio, los efectos sobre el perfil de riesgo actual y la regulación.	Se omite		
Fase 6. Responder al riesgo	Aplicar el plan de respuesta adecuado para minimizar el impacto cuando se produzcan incidentes de riesgo.	Se altera	Aplicar el plan de respuesta adecuado para minimizar el impacto cuando se produzcan incidentes de riesgo, de acuerdo a Norma NTC-ISO/IEC 27001,6.1.3	Cumplir con Numeral 7.5 de la norma ISO/IEC 27001:2013 donde la entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información
	Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.	Se omite		Estas actividades se omiten ya que el plan de acciones para el tratamiento de riesgos está en la primera actividad de esta fase, y se relaciona enteramente con el Numeral 7.5 de la norma ISO/IEC 27001:2013
	Categorizar incidentes, y comparar la exposición real respecto a los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los tomadores de decisiones en el marco de presentación de informes, y actualizar el perfil de riesgo.	Se omite		
	Examinar los eventos / pérdidas adversos pasados y la pérdida de oportunidades y determinar las causas raíz. Comunicar la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras en los procesos a los procesos de gobierno de riesgos y a los tomadores de decisiones adecuados;	Se omite		

Tabla 1: Modelo de adaptación de la fase PLAN

En la siguiente tabla 2 se observa como algunas Fases del Proceso APO12 de Cobit 5 para riesgos ayudan a alcanzar ciertos requisitos de un SGSI:

Ítem	**Requisitos para la valoración de riesgos según ISO/IEC 27001:2013**	**Cumplimiento del requisito con la metodología de valoración de riesgos Cobit 5 Para Riesgos (Proceso APO12).**
6.1.2 - c	Identifique los riesgos de la seguridad de la información: 1. Identificar los riesgos asociados con la perdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI 2. Identificar a los dueños de los riesgos	En la Fase 1 y 2 de la metodología se identifican los riesgos.
6.1.2 - d	Analice los riesgos de la seguridad de la información 1. Valorar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 - c - 1 2. Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 - c – 1 3. Determinar los niveles de riesgo	En la Fase 2 valora el impacto negativo resultante de que un escenario de riesgo se materialice. En la Fase 2 se valora la probabilidad de ocurrencia de amenazas En la Fase 2 se determina el nivel de riesgo.

Tabla 2: Cumplimiento de requisitos de la norma, aplicando COBIT 5 para Riesgos,

Se toman dos marcos de referencia, la Norma y el Proceso APO12 de Cobit 5 para Riesgos, y a continuación se hace una comparación de estas en cada una de las fases y etapas, para luego poder realizar una integración, para este paso se usó el "Método de integración para soportar la armonización de múltiples modelos y estándares" [27].

Con este método se definió los marcos de la siguiente forma:

Marco A: Fase de Plan de un SGSI basado en la norma ISO/IEC 27001:2013

Marco B: APO12 Cobit 5 para Riesgo

EP (Elemento de Proceso) del marco A: Etapas (5) del Marco A

EP (Elemento de Proceso) del marco B: Pasos (6) del Marco B

EPSI (Elementos de Proceso Sensibles a ser Integrados): Todos los EP de los marcos de referencia son EPSI.

Los criterios de integración que se utilizaron son los definidos por el autor, los criterios son los siguientes:

Criterios de Integración:

"*Cuando la descripción de un EPSI definido en un marco A está soportado y contenido en la descripción de un EPSI definido en un marco B:*

i). Cuando el EPSI del marco A ofrece una descripción más detallada que el EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A.

ii). Cuando el EPSI del marco A ofrece una descripción igual (en detalle) que la descripción del EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A o viceversa.

iii).Cuando el EPSI del marco A ofrece una descripción con menos detalle que el EPSI del marco B, el EPSI de A podría ser absorbido por el EPSI de B"

En la tabla 3 se muestra la Relación de EPSI de los marcos de referencia

Relación	EPSI Marco A	EPSI Marco B
1	• Caso de negocio y Plan de Proyecto.	
2	• Alcance, Limites y Política del SGSI	
3	• Análisis de activos de información	• Fase 1 • Fase 2
4	• Valoración de Riesgos	• Fase 2 • Fase 4
5	• Selección de objetivos de control y controles	• Fase 5
6	• Entregables	• Fase 6

Tabla 3: Relación de EPSI de los marcos de referencia.

Ahora se aplicará el proceso definido en la ilustración 16 y el resultado está definido en la tabla 4.

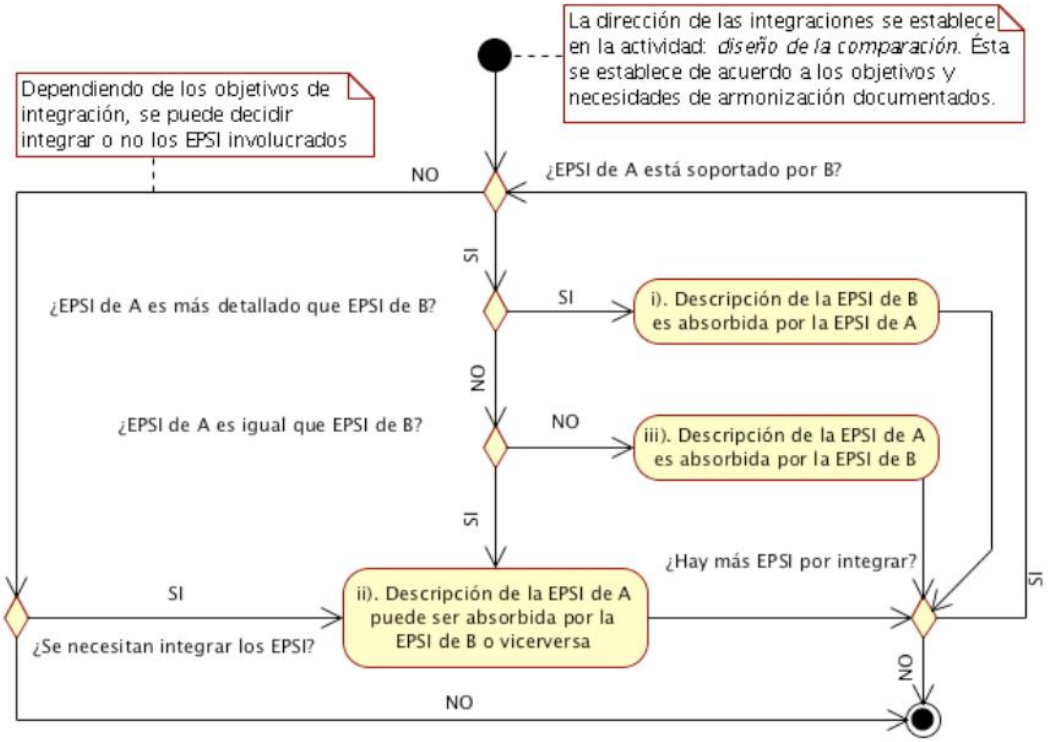

Ilustración 16: Proceso de comparación e integración

Para definir sin el EP de un marco es más detallado que el EP del otro marco, se usó la siguiente documentación.

- Para EP del Marco A: Norma ISO/IEC 27001:2013 y Guía Técnica ISO/IEC 27003:2012
- Para EP del Marco B: Guía de Cobit 5 para Riesgo Proceso APO12

EPSI Relacionados		**EP a usar según criterios de integración**	**Documentación de soporte**
Macro A	**Marco B**		
Caso de negocio y Plan de Proyecto.		Caso de negocio y Plan de Proyecto.	Numeral 4.1 a 4.3 de la norma ISO/IEC 27001:2013
Alcance, Limites y Política del SGSI		Alcance, Limites y Política del SGSI	Numeral 5 y 6 de la GTC ISO/IEC 27003:20112
Análisis de activos de información		Análisis de activos de información	Numeral 7.3 de la GTC ISO/IEC 27003:2012
Valoración de Riesgos	Fase 1	Fase 1	Fase 1 de Cobit 5 APO12.1
	Fase 2	Fase 2	Fase 2 de Cobit 5 APO12.2
	Fase 4	Fase 4	Fase 2 de Cobit 5 APO12.4
Selección de objetivos de control y controles	Fase 5	Selección de objetivos de control y controles	Numeral 6.1.2 de la norma ISO/IEC 27001:2013
			Numeral 8.3 de la GTC ISO/IEC 27003:2012
Información Documentada	Fase 6	Información Documentada	Numeral 7.5 de la norma ISO/IEC 27001:2013

Tabla 4: Integración de marcos de referencia

Con estos resultados se determina cuáles son los EP a usar en la adaptación de Cobit 5 para Riesgos.

Finalmente se muestra en la ilustración 17. Adaptación de la Metodología de Valoración de Riesgos completa, luego de la adaptación del Proceso APO12 que se propuso, cumpliendo con la norma la norma ISO/IEC 27001, siguiendo la ISO/IEC 27003 como guía de implementación.

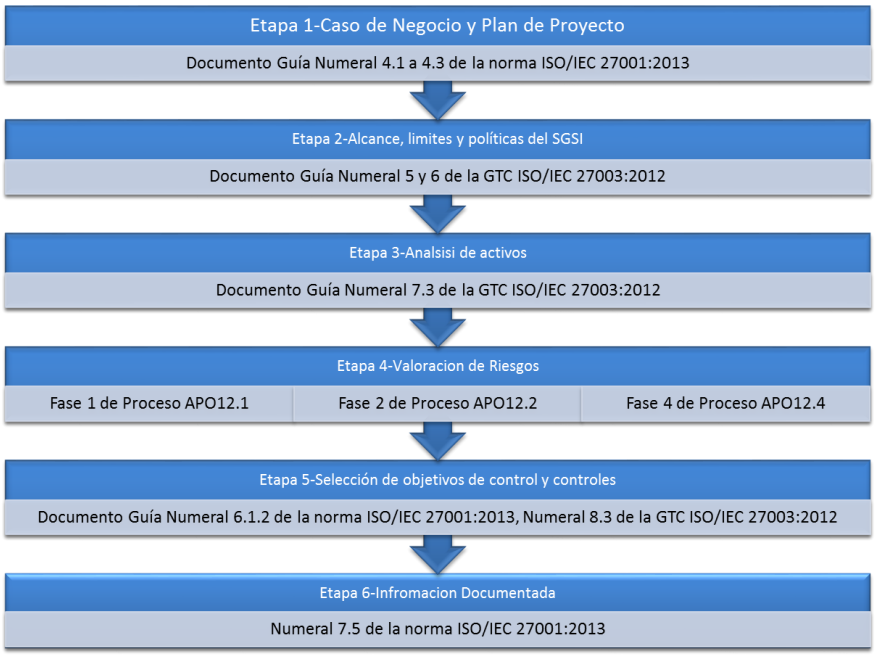

Ilustración 17: Adaptación de la Metodología de valoración de riesgos.

Descripción de cada etapa:

- Etapa 1. Caso de Negocio y Plan de Proyecto: Establecer los criterios básicos necesarios para la gestión de riesgos y seguridad de la información con la empresa, establecer un cronograma y costos así como los requisitos legales y reglamentarios. Y las obligaciones contractuales.
- Etapa 2. Alcance Límites y Política del SGSI: Es necesario Definir el alcance y los límites de la gestión de riesgo en la seguridad de la información, para entender los aspectos internos y externos a tener en cuenta, así mismo como crear las políticas.
- Etapa 3. Análisis de activos: Realizar una lista detallada de los activos que se identificaron dentro del alcance y su respectiva tasación para encontrar los más importantes para la organización.
- Etapa 4. Valoración de Riesgos: Identificar, valor, amenazas y escenario de riesgo estimándolos mediante frecuencia e impacto y uso de mapa de riesgo.
- Etapa 5. Selección de objetivos de control y controles: Tratamiento para los riesgos identificados y seleccionar controles para los aquellos que se van a mitigar.
- Etapa 6. Información Documentada: toda la Información detallada de la fase plan del SGSI.

5. PROCESO METODOLOGICO EN BASE A LA NORMA ISO/IEC 27001 SIGUIENDO LA ISO/IEC 27003.

ISO/IEC 27001 es un estándar para la seguridad de la información, el cual especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información SGSI.

Desarrolla el marco normativo, es necesario para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27000, para dicho desarrollo, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad. La ilustración 18, muestra con detalle el modelo PDCA enmarcado en la norma ISO/IEC 27001.

A continuación en la elipse roja, se resaltan los pasos tenidos en cuenta para efecto de este trabajo de grado, en la implementación del Sistema de Gestion de Seguridad de la Información, basado en la norma ISO/IEC 27001, siguiento la norma ISO/IEC 27003.

La elipse azul indica la valoracion de riesgos que se analiza en la seccion 5.4 mediante COBIT 5 como metodologia de valoracion de riesgos.

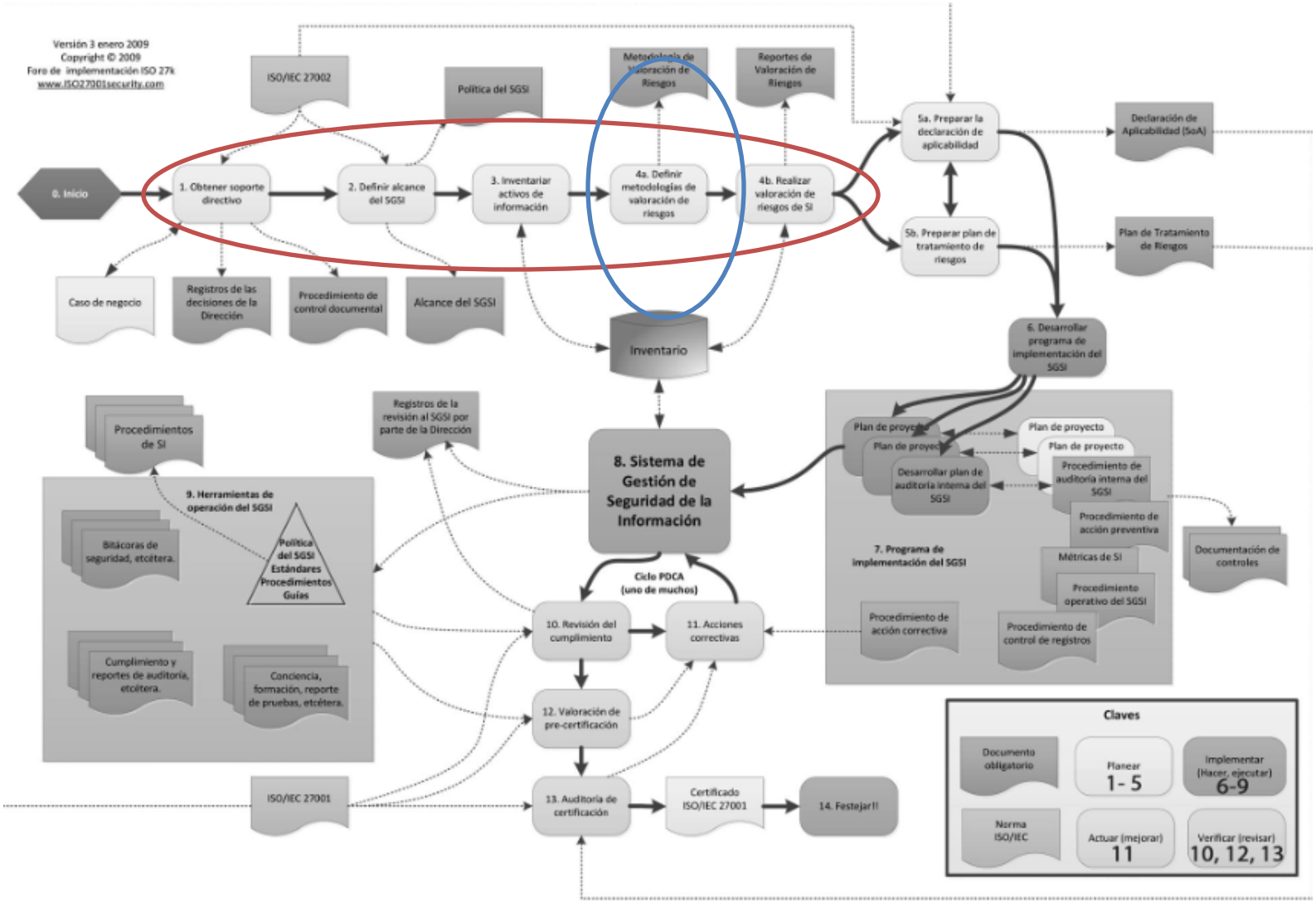

Ilustración 18: Implementación de la fase plan

5.1. OBTENER EL SOPORTE DIRECTIVO

Para obtener el soporte por medio de la dirección, se presentó a la Vicerrectoría Administrativa de la Universidad del Cauca la propuesta de implantar la fase plan de un Sistema de Gestión de Seguridad de la Información SGSI al Área de Recaudos de la División de Gestión Financiera soportado por la Resolución número 005 de 2015 (7 de enero) [anexo A], lo anterior a solicitud del Rector delegatorio de la Universidad del Cauca, obteniendo así el consentimiento por parte de la vicerrectoría, quien permite el acceso a la División de Gestión Financiera y a la División de las TIC, realizando la respectiva autorización a los jefes y personal encargado de estas dependencias (para la División de Gestión Financiera, es el técnico administrativo del área de Recaudos y para la División de las TIC, el ingeniero encargado de los servidores de la Universidad), quienes suministraran la información necesaria en el desarrollo..

5.1.1. Caso de Negocio

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo, por lo tanto se requiere de una gestión efectiva de la seguridad en la cual debe tomar parte activa el área de recaudos, dirigida por el Técnico Administrativo, además debe tomar en consideración a la comunidad universitaria y proveedores de bienes y servicios.

Con la implementación de un SGSI, la División conoce los riesgos a los que está sometida su información, lo cual le permite asumir, minimizar, transferir o controlarlos mediante un sistema definido, documentado y conocido que se revisa y mejora constantemente.

Para llevar a cabo este proceso se deben tener en cuenta las metas y objetivos establecidos por la Universidad del Cauca, como son definir la estructura organizacional y los recursos necesarios para la implantación de un Sistema de Gestión de Seguridad de la Información; cuya meta principal, es la Certificación de un SGSI, el cual es un proceso mediante el que una Entidad de Certificación externa, independiente y acreditada, audita el sistema determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia, y en caso positivo emite el correspondiente certificado.

Los beneficios que conlleva la implantación de un SGSI para la Universidad del Cauca, se enmarca en:

- Reducción de Costos: disminución de las primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados, o evitando indemnizar a usuarios por malas gestiones.

- Mantener y mejorar la imagen: la comunidad universitaria percibirá a la División de Gestión Financiera, en consideración al área de Recaudos como una entidad responsable, comprometida con la mejora de sus procesos y servicios. Así mismo, reconociéndola como una División consolidada y de confianza, que facilita la gestión general y habilita nuevas posibilidades para la toma de decisiones.
- Cumplimiento legal y reglamentario: la Universidad del Cauca con la implementación del SGSI estará dando cumplimiento al marco normativo establecido en decretos, leyes y resoluciones estipuladas por el gobierno nacional (MinTic) [28][29].

5.1.2. Registros de las Decisiones de la Dirección

Las decisiones tomadas por la Dirección están soportadas por documentos firmados y aceptados para la implantación del SGSI (anexo B), de esta manera los miembros encargados de este proceso pueden adquirir toda la información necesaria; esto es permitido por medio de un documento de confidencialidad autenticado por notaria (anexo C) en el cual compromete a los miembros encargados de la organización a la no divulgación de ningún tipo de información, debido a que para la Universidad es de mucho valor y puede representar un alto índice de riesgo. Posteriormente el jefe de la división autorizo y permitió tener acceso a toda la información (anexo D).

5.1.3. Procedimiento de control documental

Se realiza por medio del archivo de actas correspondientes a las reuniones (anexo E) con el técnico administrativo y el jefe de la División de Gestión Financiera, de igual manera con el Ingeniero encargado de la División de las TIC, los cuales brindan la información necesaria para la implantación del SGSI, como también de la verificación y aceptación de los avances presentados en las reuniones establecidas.

5.2. DEFINIR EL ALCANCE DEL SGSI, SUS LÍMITES Y SUS POLÍTICAS

Para definir el alcance del SGSI para la División, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión, es importante que se definan los límites del SGSI, y se cree un diagrama donde se expongan los procesos y procedimientos que serán objeto de análisis. Además se deben definir claramente los organigramas, para tener los objetivos claros y cumplir los requisitos a través de criterios y estrategias para evaluar el riesgo.

5.2.1. Alcance y límites del SGSI.

Se debe definir el alcance de un SGSI de manera que comprenda toda la organización o a una parte de ella tal como una división o una subdivisión claramente delimitada. Teniendo en cuenta lo anterior es posible la definición del alcance en el área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca.

5.2.1.1. Definir el alcance y los límites de las tecnologías de la información y telecomunicaciones.

Los límites de las TIC son:

- Problemáticas técnicas: incompatibilidades entre diversos tipos de ordenador y sistemas operativos.
- Falta de información: las necesidades de conocimientos teóricos y prácticos que todas las personas deben aprender, la necesidad de aptitudes y actitudes favorables a la utilización de nuevas y existentes herramientas manejadas en la división.
- Problemas de seguridad: riesgo de accesos no autorizados a los ordenadores de alguna entidad que están conectados a internet y el posible robo de códigos o claves con las que se tengan acceso a información.
- Barreras económicas: el abaratamiento de los equipos y programas informáticos
- Barreras culturales: el idioma dominante correspondiente al inglés, en el que se encuentran muchas referencias e información de internet; también la tradición en el uso de instrumentos tecnológicos avanzados

5.2.1.2. Definir el alcance y límites físicos.

Se presentan riesgos físicos como incendios, inundaciones, terremotos o vandalismo que pueden afectar la disponibilidad de la información y los recursos, haciendo inviable la continuidad de la institución si no cuenta con acciones adecuadas para afrontarlos.

La descripción de la organización y sus características geográficas evidenciando el alcance interno y externo dentro de la División de Gestión financiera de la Universidad del Cauca se encuentra descrita de la siguiente manera:

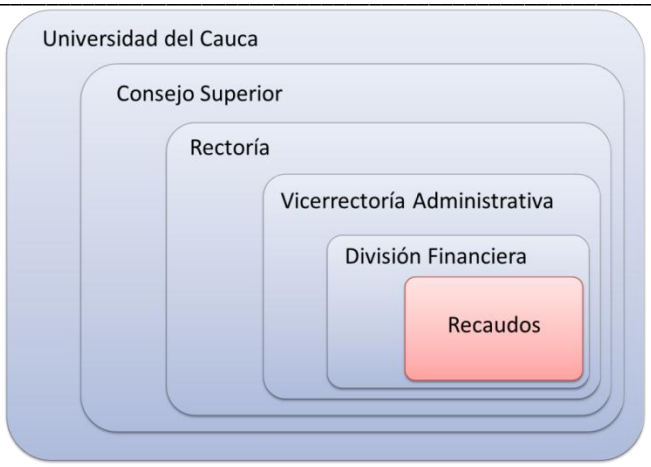

Ilustración 19: Organización física del área de recaudos

- **Ubicación Física del Área de Recaudos.**

La ubicación de la división de Gestión Financiera, en donde se encuentran las oficinas con el personal encargado se encuentra localizada en la calle 4 # 5 - 30, Centro histórico de la ciudad de Popayán, Cauca.

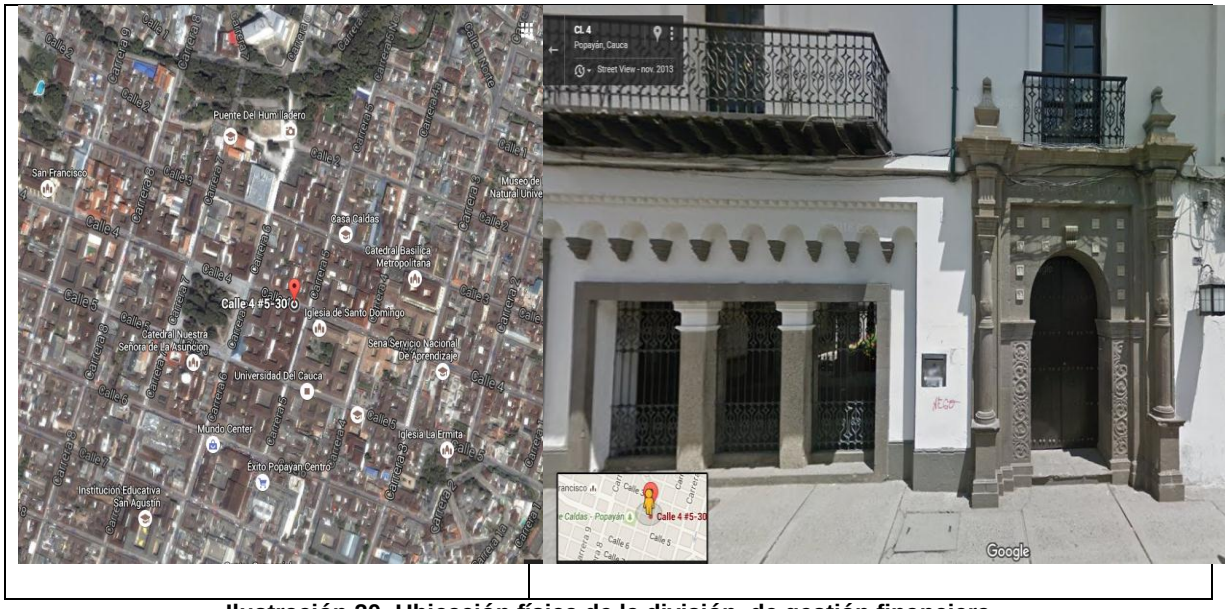

Ilustración 20: Ubicación física de la división de gestión financiera

Las oficinas especiales, utilizadas para almacenar o contener el hardware de las TIC o los datos dentro del alcance basándose en las limitaciones de las TIC, se encuentran ubicada en la Facultad de Ciencias Naturales, Exactas y de la Educación- Campus Tulcán en la dirección calle 2 No. 3N-100, de la ciudad de Popayán- Cauca ver ilustración 22, en la cual están todas las instalaciones de la División de las TIC de la Universidad del Cauca.

Ilustración 21: Campus de la facultad de Ciencias Naturales, Exactas y de la Educación

5.2.1.3. Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI.

Luego de tener consolidada toda la información para integrar cada alcance, se utilizó la metodología de las Elipses siguiendo el estándar ISO 27001, que exige como punto de partida establecer el SGSI y definir el "alcance del SGSI" en términos de las características de la dependencia, ubicación, activos y tecnología.

El método de las elipses, permite inicialmente distinguir a la División de Gestión Financiera los procedimientos con sus respectivas actividades y a cada proceso identificarle su respectivo subprocesos.

Los nueve procedimientos con los cuales cuenta la División de Gestión financiera son los siguientes:

1. Conciliaciones Bancarias y Saldos de Tesorería y Contabilidad.
2. Declaraciones Tributarias.
3. Egresos por Devoluciones y Descuentos.
4. Egresos Presupuestales.
5. Legalización de Comisión y Avance.
6. Modificaciones Presupuestales.
7. Plan Anual de Caja PAC.
8. Recaudos.
9. Estados Financieros.

El método de las elipses (Ilustración 22) permite determinar los procedimientos de la División de Gestión Financiera que conforman el proceso, a cada procedimiento se le identifican sus respectivos procedimientos ; en la elipse intermedia, se determinan las diferentes relaciones que los procedimientos de la elipse

concéntrica tiene con otros procesos de la Universidad del Cauca; y finalmente en la elipse externa, se resaltan aquellas organizaciones que no hacen parte de la Universidad del Cauca pero tienen algún tipo de interacción con los procesos y subprocesos de la elipse concéntrica.

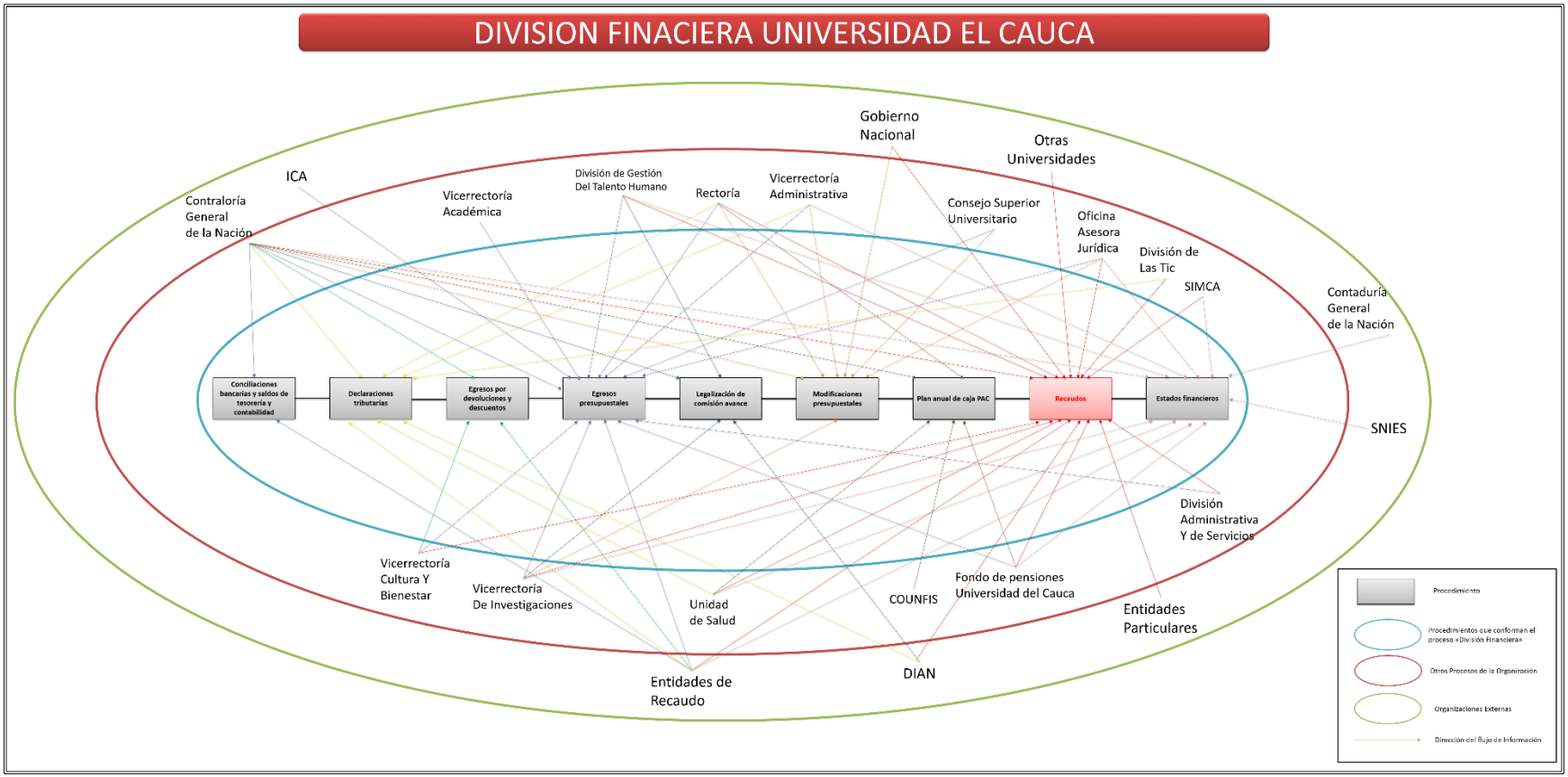

Ilustración 22: Elipse de la división de gestión financiera

Dado lo anterior, el procedimiento de Recaudos es considerado de mayor criticidad, esto también reflejado en la resolución número 005-de 2015 (7 de enero) (Anexo A). También, se evidencia que en la División de Gestión financiera, más específicamente en el Procedimiento de Recaudos se relaciona con muchas dependencias lo cual se estableció que cuenta con información crítica, esto debido a que es una fuente primaria de información institucional, por tanto este procedimiento requiere de la implantación del Sistema de Gestión de Seguridad de la Información; teniendo en cuenta su función principal.

Los anteriores resultados se obtuvieron gracias a la información brindada por el técnico administrativo de la División Financiera quien realizó ciertas aclaraciones respecto a algunas de las actividades de los procedimientos que fueron modificadas, aclaradas y agregadas (anexo E: acta 2 y 3).

5.2.2. Políticas del SGSI.

Las políticas de seguridad que soportan el sistema de gestión de seguridad de la información SGSI de la División de Gestión Financiera son basadas en las políticas estipuladas por la Universidad del Cauca según la resolución R-785 [30], de donde se determinan las políticas de la división y las cuales son:

1. La Universidad del Cauca y en especial la División de Gestión Financiera, ha decidido definir implementar y operar de manera continua un Sistema de Gestión de Seguridad de la Información-SGSI, de acuerdo a las necesidades de la División de Gestión Financiera.
2. La División de Gestión Financiera protegerá la información generada, procesada o resguardada de todos sus procedimientos, su infraestructura tecnológica y sus activos de riesgo que se generen dentro de esta.
3. La División de Gestión Financiera protegerá la información creada, procesada, transmitida o resguardada por sus procedimientos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la información.
4. La División de Gestión Financiera protegerá las instalaciones de procesamiento y la infraestructura, las cuales soportan los procesos de la institución.
5. La División de Gestión Financiera implantará controles de acceso a la información, sistemas y recursos de las redes de datos.
6. La División de Gestión Financiera garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas para garantizar la seguridad de la Información.

Las políticas expuestas fueron analizadas y aceptadas por el jefe de la División de Gestión Financiera, el cual dio su aprobación indicando que se ajustaban para la

división (Anexo E). Estas políticas fueron creadas basándose en las adoptadas por la Universidad del Cauca, las cuales son requeridas por "Controles de seguridad_ Modelos de Seguridad de la información para la Estrategia de Gobierno en línea" [31].

5.3. INVENTARIO ACTIVOS DE INFORMACIÓN.

Los activos de información que conforman los servicios que proveen las entidades para la Estrategia de Gobierno en línea son activos públicos y por lo tanto, deben protegerse adecuadamente, para esto deben ser clasificados según la necesidad, las prioridades y grado de protección esperado en el manejo de los mismos.

Los diferentes activos de información se identifican y se determinan respondiéndose a las siguientes preguntas de la Tabla 5:

Preguntas	Respuestas
¿Qué sistemas el personal de Recaudos necesitan para realizar su trabajo?	Oficina cómoda, mesa grande y cómoda, un equipo de cómputo, radioteléfono, los servidores que contenga las plataformas de SIMCA, SQUID, FINANZAS PLUS.
¿Qué información el personal de Recaudos necesitan para realizar su trabajo?	Recibe la información obtenida del administrador del SQUID y la administración de SIMCA sobre los actos que fijan tasas y directrices en materia de recaudo. Requiere de la copia de los comprobantes de consignación por reintegros o retenciones aplicados en pagos con avances para ser anexadas a la relación.
¿Qué aplicaciones el personal de Recaudos necesitan para realizar su trabajo?	Correo electrónico institucional, sistema integrado de recaudo (SQUID), base de datos de personas inscritas en la Universidad, SIMCA, FINANZAS PLUS.
¿Qué servicios el personal de Recaudos necesitan para realizar su trabajo?	Energía eléctrica, servicio de internet, red interna, iluminación planta eléctrica, red telefónica.
¿Qué personas tienen una habilidad especial o conocimiento que es vital para su organización y sería difícil de reemplazar? ¿Qué habilidades tienen estas personas?	Ingeniero de soporte (desarrollo), Técnico administrativo (conocer el proceso y reglamentación institucional), profesional universitario (conocer el proceso y reglamentación institucional).
¿Qué activos intangibles el personal de Recaudos necesita para realizar su trabajo?	Reputación e imagen.

Tabla 5: Identificación de activos

Es importante analizar la situación actual en la que se encuentra la organización, ya que es recomendable considerar los requisitos y activos de información existentes al implementar un SGSI.

Para no comprometer la seguridad de la División y analizando la tabla anterior, la lista de activos de información que se identifica en el área de Recaudos de la división de gestión financiera se encuentran en el anexo (Anexo: F).

5.3.1. Categorización de activos a nivel de Información, Software, Hardware y de Servicios

Los activos de información son manejados por los funcionarios de la División de Gestión Financiera a través del procedimiento Recaudos, con el fin principal de determinar qué activos posee el área, reconocer el valor de cada uno, los niveles de acceso permitidos y determinar su clasificación para que sea utilizada adecuadamente.

La clasificación se hace de la siguiente manera:

- Servicio.
- Datos / Información.
- Aplicaciones (Software).
- Equipos informáticos (Hardware).
- Redes de Comunicaciones.
- Soportes de Información.
- Equipamiento Auxiliar.
- Instalaciones.
- Personal.

La lista de activos completa con su respectiva definición y clasificación se encuentra en el anexo (Anexo: G).

5.3.2. Tasación de activos.

En esta etapa, se lleva a cabo un análisis de los activos identificados como vitales del proceso anterior, sin embargo para poder identificar la protección apropiada de estos, es necesario tasar su valor en términos de la importancia a la gestión de la información; de igual manera, para valorar y priorizar los activos de información, es importante otorgarles un valor de confidencialidad, integridad y disponibilidad, esto según la definición dada en el capítulo I.

Con lo mencionado anteriormente, para la tasación de activos, se manejó una escala de Likert, en dónde el valor 1 significa “muy poco” y 5 “muy alto”. En este punto, se podría efectuar la siguiente pregunta ¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad? O de igual manera ¿Qué importancia tiene el activo para el área de Recaudos de la Universidad del Cauca? Esta fuente de tasación es tomada de Alberto G. Alexander.

- Confidencialidad:

Escala	Criterio
5	Muy alto
4	Alto
3	Medio
2	Poco
1	Muy poco

Tabla 6: Tasación de confidencialidad

- Integridad.

Escala	Criterio
5	Muy alto
4	Alto
3	Medio
2	Poco
1	Muy poco

Tabla 7: Tasación de Integridad

- Disponibilidad.

Escala	Criterio
5	Muy alto:
4	Alto
3	Medio
2	Poco
1	Muy poco

Tabla 8: Tasación de Disponibilidad

En las Tablas 6, 7 y 8 se observa la definición de los valores a los criterios de confiabilidad, integridad y disponibilidad, de los cuales se hace la respectiva valoración de activos. Con los valores obtenidos de las anteriores definiciones se encuentra la criticidad, obtenida mediante un promedio de valores de los criterios anteriores los cuales dan valor y prioridad a los activos de información.

La tabla 9 muestra la escala de Criticidad obtenida para los activos de información.

Criticidad	
Escala	**Criterio**
5	Muy alto
4	Alto
3	Medio
2	Poco
1	Muy poco

Tabla 9: Tasación de Criticidad

En el anexo (anexo H), determina el nivel promedio actual de seguridad en el área de Recaudos, estos resultados son obtenidos por parte del técnico administrativo de la

división financiera como también del ente encargado en la división de las TIC de la Universidad del Cauca.

5.3.3. Identificación de Amenazas y Vulnerabilidades

5.3.3.1. Identificación de Amenazas.

Los activos de información de Recaudos, están sujetos a distintas formas de amenazas, las cuales pueden causar un incidente no deseado que genere daño a la División y a sus activos.

A continuación en la tabla 10, se presentan las amenazas seleccionadas que se encuentran presentes en el área de Recaudos; esta tabla es tomada del anexo C de ISO/IEC 27005:2008 [32].

D: Deliberadas (D) A: Accidentales (A) E: Ambientales (E)

TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	A,D,E
	Daño por agua	A,D,E
	Contaminación	A,D,E
	Accidentes importantes	A,D,E
	Destrucción de equipo o los medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
Eventos Naturales	Fenómenos Climáticos	E
	Fenómenos Sísmicos	E
	Fenómenos Volcánicos	E
Pérdida de servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado.	A,D
	Perdida de suministro de energía	A,D,E
	Falla en el equipo de telecomunicaciones	A,D
Perturbaciones por radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Pulsos electromagnéticos	A,D,E
Exposición de la información	Interpretación de señales de interferencia comprometedoras.	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipos	D
	Recuperación de medios reciclados o desechados	D
	Divulgación de información	A,D
	Datos provenientes de fuentes no confiables	A,D
	Manipulación con hardware	D
	Manipulación con software	A,D
	Detección de la ubicación	D
Fallas técnicas	Falla en equipos	A
	Mal funcionamiento del equipo	A
	Saturación del Sistema de Información	A,D

	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso no autorizado de equipos	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A,D
	Corrupción de datos	D
	Procesamiento ilegal de los datos	D
Compromiso de funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A,D,E

Tabla 10: Amenazas comunes ISO/IEC 27005

5.3.3.2. Identificación de Vulnerabilidades

Al tratar de definir las vulnerabilidades en Recaudos, la mejor manera es pensar en las debilidades del sistema de seguridad, asociadas con los activos de información del área en cuestión.

A continuación, se presenta en la tabla 11, las amenazas que pueden explotar estas vulnerabilidades, las cuales fueron seleccionadas de acuerdo al área de Recaudos; esta tabla es tomada del anexo D de ISO/IEC 27005.

Tipos	Vulnerabilidades	Amenazas
Hardware	Mantenimiento insuficiente/ instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Susceptibilidad a la húmeda, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos.
	Copia no controlada	Hurto de medios o documentos.
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Ausencia de “Terminación de la sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
Software	Asignación errada de los derechos de acceso	Abuso de los derechos
	En términos de tiempo utilización de datos errados en los programas aplicación	Corrupción de datos
	Ausencia de mecanismos de identificación y autentificación, como la autenticación del usuario.	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Ausencia de copias de respaldo	Manipulación de software
Red	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor receptor	Falsificación de derechos
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disposición del

		personal
	Uso incorrecto de software y hardware	Error en el uso
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medio o documentos
	Entrenamiento insuficiente de seguridad	Error de uso
Lugar	Uso inadecuado o destrucción del control de acceso físico a las edificaciones y mensajería.	Destrucción de equipos o medios
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipos
Organización	Ausencia de procesamientos de monitoreo de los recursos de procesamientos de información	Abuso de derechos
	Ausencia de procesamientos de identificación y valoración de riesgos	Abuso de derechos
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de mecanismo de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos.

Tabla 11: Listado de ejemplos de vulnerabilidades y amenazas

En el anexo (Anexo I) se determina el listado de las posibles amenazas y vulnerabilidades, identificando sus respectivos activos de información que existen en el área de Recaudos de la División de Gestión Financiera.

5.4. METODOLOGÍA PARA LA GESTIÓN DE RIESGO

El proceso de Gestión de Riesgos APO12 de COBIT 5 para Riesgos, por medio de sus prácticas, permite establecer el análisis de riesgos identificado en la ilustración 12 del capítulo 4; el cual consiste en recolectar datos, analizar el riesgo, mantener un perfil de riesgo, expresar el riesgo, definir un portafolio de acciones para la gestión del riesgo y responder al riesgo.

5.4.1. Recolectar datos

Para la identificación, recolección de datos y posterior análisis se hizo una investigación a fondo conociendo el procedimiento del área de recaudos, a través de reuniones (Anexo E), encuestas (Anexo J) y siguiendo la norma ISO/IEC 27003 de la siguiente forma:

- Obtener la aprobación de la dirección para iniciar un proyecto SGSI.
- Definir el alcance y los límites de la organización.
- Realizar un análisis de los requisitos de seguridad de la información.

Con esto se logró identificar las condiciones que existen cuando se materializa un riesgo y como este puede afectar la realización del procedimiento, y se ejecutó un análisis del medio para verificar los factores de riesgo.

De acuerdo con la información obtenida se han identificado los siguientes riesgos:

Riesgos Encontrados			
1	Ausencia total de políticas de TI, por lo que el personal no está capacitado en el cumplimiento de estas	**6**	No existen acuerdos de confidencialidad de la información que se maneja
2	falta de preparación en caso de riesgos que se puedan presentar, ya que no se conocen las amenazas y vulnerabilidades en la entidad	**7**	Total dependencia de personal para tareas de suma importancia en la entidad
3	Falta del conocimiento en TI, por lo que no se cumple muchos de los aspectos que la ley y las buenas prácticas en seguridad dictan	**8**	No se realizan evaluaciones periódicas que identifiquen riesgos y vulnerabilidades en el sistema y en el personal
4	Intercambio de información sin controles que permitan un nivel de riesgo toreable, ya que no existe un proceso o forma que lo respalde	**9**	Interrupción total de comunicación entre la división financiera y los servidores donde se aloja la información por daños maliciosos en la red de comunicación
5	No existen protocolos obligatorios de cambio de claves y de cierre de sistemas que otorguen un adecuado acceso a la información	**10**	Privilegios de usuario que permiten modificar información sin dejar un rastro que lo respalde

Tabla 12: Riesgos Encontrados

- **Identificación de los procesos:**

Cobit 5 utiliza un modelo de procesos de mejora continua que ayuda a las metas TI las cuales aseguran el cumplimiento de las metas empresariales, manteniendo así un nivel operativo que verifica el valor de la entidad.

A continuación se crearan tres objetivos relacionados directamente con la seguridad de la información, políticas, activos y riesgo, que van ligados a los objetivos de esta tesis, de esta forma posteriormente identificar las metas empresariales y las metas TI, que nos llevaran a encontrar los procesos planteados en COBIT 5 y que al final ayudaran a entender donde se están generando los riesgos y como se pueden estos abordar con los escenarios de riesgos de la plantilla de Cobit 5 Para Riesgos.

1. *Mejorar y mantener las habilidades del personal de tal forma que su conocimiento vaya enfocado en el desempeño de actividades relacionadas con las Tecnologías de la Información.*

Se bebe de educar al personal en TI para que tenga una mayor productividad, mediante la realización de capacitaciones y actividades que mejoren sus habilidades, adquieran buenas prácticas y desarrollen metodologías para el desarrollo e implantación de software.

2. *Mejorar la infraestructura de TI disponible mediante la optimización de costos que permitan invertir en medidas de seguridad para de esta forma conseguir los diferentes objetivos y metas planteadas en la entidad.*

Consiste en permitir la protección y salvaguardar la información confidencial gracias al mejoramiento y actualización de la infraestructura que se maneja en la entidad, así como actualización de software y cambio de equipos obsoletos, todo esto a través de la optimización de los costos.

3. *Identificar, analizar, evaluar y reducir los riesgos en la entidad a través de la implementación de un sistema de seguridad de la información que cumpla las políticas internas.*

Se enfoca directamente en la creación de un SGSI, que identifique activos y escenarios de riesgo, así como evaluarlos y crear un plan estratégico para la respuesta a los riesgos, se deben crear políticas de seguridad que cumplan con la normativa interna y externa.

- **Identificación de metas corporativas**

Con los objetivos identificados, se debe determinar las metas corporativas genéricas que tiene COBIT 5 teniendo en cuenta la situación específica de la entidad, relacionando y comparando los objetivos y las metas y refinándolas para que se adecuen a las cascada de metas de COBIT 5.

Dimensión de CMI		Meta Corporativa
Financiera	1	Valor para las partes interesadas de las inversiones de Negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de Leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto negocio

Tabla 13: Metas Corporativas

Las metas corporativas genéricas de COBIT 5 se dividen en:

1. FINANCIERA: mejorar y aumentar los beneficios de inversión al fin de evitar pérdidas y optimizar los costos.
2. CLIENTE: relacionada satisfacer al cliente de la entidad.
3. INTERNA: centrada en la productividad, los procesos, normativa entre otros dentro de la entidad, mejora su funcionamiento.
4. APRENDIZAJE Y CRECIMIENTO: relaciona directamente al personal y le da la importancia necesaria para mejorar la entidad.

Estas metas corporativas han sido desarrolladas utilizando las dimensiones del cuadro de mando integral (CMI. En inglés: Balanced Scorecard, BSC) y representan una lista de objetivos comúnmente usados que una empresa puede definir por sí misma [33].

Para el mapeo de las metas corporativas genéricas con respecto a los objetivos se tomaron cada uno de ellos y se asignaron a cada una de las metas de la siguiente forma:

Objetivo 1. Mejorar y mantener las habilidades del personal de tal forma que su conocimiento vaya enfocado en el desempeño de actividades relacionadas con las Tecnologías de la Información.

Al mapear los objetivos con las metas genéricas de Cobit 5, con el objetivo 1, se determinó que las Metas Corporativas que se relacionan directamente con este son:

Dimensión de CMI		Meta Corporativa
Financiera	1	Valor para las partes interesadas de las inversiones de Negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de Leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto negocio

Tabla 14: Metas Corporativas/ objetivo 1

- *14: Productividad operacional y de los empleados*
- *16: Personas preparadas y motivadas.*

El objetivo va enfocado en mejorar la preparación y la productividad en el personal a través de la estructuración de un área capacitada en TI, que brinde el soporte y optimice los costos de los recursos que se manejan, por eso se toman en cuenta estas dos metas empresariales que Cobit 5 sugiere, una va enfocada directamente con la parte interna de la entidad que se relaciona con el adecuado desarrollo de las labores de los empleados, y la otra con el aprendizaje de estos para que su formación este actualizada y de buena calidad.

Objetivo 2. Mejorar la infraestructura de TI disponible mediante la optimización de costos que permitan invertir en medidas de seguridad para de esta forma conseguir los diferentes objetivos y metas planteadas en la entidad.

Al mapear los objetivos con las metas genéricas de Cobit 5 con el objetivo 2, se determinó, que las Metas Corporativas que se relacionan directamente con este son:

Dimensión de CMI		Meta Corporativa
Financiera	1	Valor para las partes interesadas de las inversiones de Negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de Leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto negocio

Tabla 15: Metas Corporativas/ objetivo 2

- *12: Optimización de los costes de los procesos de negocio.*
- *15 Cumplimiento con las políticas internas*

Al mejorar el presupuesto del área y reducir costos se puede contemplar una diversidad de alternativas que permitan asignar los recursos al mejoramiento de la infraestructura que se posee dando cumplimiento a las políticas internas de la entidad, de la misma forma estas políticas contribuyen directamente en la realización de los objetivos y metas que se están planteando al interior de la entidad.

Objetivo 3. Identificar, analizar, evaluar y reducir los riesgos en la entidad a través de la implementación de un sistema de seguridad de la información que cumpla las políticas internas.

Al mapear los objetivos con las metas genéricas de Cobit 5 con el objetivo 3, se determinó, que las Metas Corporativas que se relacionan directamente con este son:

Dimensión de CMI		Meta Corporativa
Financiera	1	Valor para las partes interesadas de las inversiones de Negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de Leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto negocio

Tabla 16: Metas Corporativas/ objetivo 3

- *3: Riesgos de negocio gestionados (salvaguarda de activos)*
- *15: Cumplimiento con las políticas internas*

Para el desarrollo de este objetivo se tuvo en cuenta estas dos metas empresariales ya que va directamente enfocada en la gestión del riesgo del negocio y la protección de los activos de información, así mismo el cumplimiento de políticas internas que van relacionadas con reducir el nivel de riesgo y aumentar la seguridad en la entidad.

- Identificación de las metas de TI

Luego de identificar cada una de las metas empresariales, se debe identificar a través de la tabla (Anexo: K) que Cobit 5 propone las metas de TI, las cuales serán mapeadas para posteriormente identificar los procesos.

Para la ubicación de dichas metas, primero se localizan las Metas Corporativas y se sigue en forma descendente hasta encontrar un “P” o una “S”, de esta forma se intercepta la meta corporativa con la Meta TI, la “P” indica que la Meta apoya totalmente la meta corporativa y la “S” sirve de un apoyo secundario.

<u>Objetivo 1: Mejorar y mantener las habilidades del personal de tal forma que su cocimiento vaya enfocado en el desempeño de actividades relacionadas con las tecnologías de la Información.</u>

			Metas Corporativas																			
			01. Valor para las partes interesadas de las Inversiones de Negocio	02. Cartera de productos y servicios competitivos	03. Riesgos de negocio gestionados (salvaguarda de activo)	04. Cumplimiento de leyes y regulaciones externas	05. Transparencia financiera	06. Cultura de servicio orientada al cliente	07. Continuidad y disponibilidad del servicio de negocio	08. Respuestas ágiles a un entorno de negocio cambiante	09. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación del producto y del negocio
Metas Relacionas con las TI			**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	1	Alineamiento de TI y estrategia de negocio	P	P	S			P	S	P	P	S	P		P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S						S	S	S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y fiable para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Tabla 17: Relación Metas TI/ Metas Corporativas objetivo 1

Las Metas de TI seleccionadas para este objetivo son:

La Meta Corporativa número 18: Productividad operacional y de los empleados, se relaciona directamente con:

- ✓ CLIENTE: meta número 8: uso adecuado de aplicaciones, información y soluciones de tecnología.

La Meta Corporativa número 18: personas preparadas y motivadas, se relaciona directamente con:

- ✓ APRENDIZAJE: meta número 16: personal de negocio y de las TI competente y motivado

<u>Objetivo 2. Mejorar la infraestructura de TI disponible mediante la optimización de costos que permitan invertir en medidas de seguridad para de esta forma conseguir los diferentes objetivos y metas planteadas en la entidad</u>

			Metas Corporativas																		
			01. Valor para las partes interesadas de las Inversiones de Negocio	02. Cartera de productos y servicios competitivos	03. Riesgos de negocio gestionados (salvaguarda de activo)	04. Cumplimiento de leyes y regulaciones externas	05. Transparencia financiera	06. Cultura de servicio orientada al cliente	07. Continuidad y disponibilidad del servicio de negocio	08. Respuestas ágiles a un entorno de negocio cambiante	09. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación del producto y del negocio
Metas Relacionas con las TI			**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	1	Alineamiento de TI y estrategia de negocio	P	P	S			P	S	P	P	S	P		P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y fiable para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Tabla 18: Relación Metas TI/ Metas Corporativas según objetivo 2

Las Metas de TI seleccionadas para este objetivo son:

La Meta Corporativa número 19: Optimización de los costes de los procesos de negocio, se relaciona directamente con:

- ✓ FINANCIERA: meta número 5: realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.
- ✓ FINANCIERA: meta número 6: transparencia de los costes, beneficios y riesgos de las TI.
- ✓ INTERNA: meta número 11: optimización de activos, recursos y capacidades de las TI.

La Meta Corporativa número 19: cumplimiento con las políticas internas, se relaciona directamente con:

- ✓ FINANCIERA: meta número 2: cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
- ✓ INTERNA: meta número 10: seguridad de la información, infraestructura de procesamiento y aplicaciones.

- ✓ INTERNA: meta número 15: cumplimiento de las políticas internas por parte de las TI.

Objetivo 3. Identificar, analizar, evaluar y reducir los riesgos en la entidad a través de la implementación de un sistema de seguridad de la información que cumpla las políticas internas.

			Metas Corporativas																		
			01. Valor para las partes interesadas de las Inversiones de Negocio	02. Cartera de productos y servicios competitivos	03. Riesgos de negocio gestionados (salvaguarda de activo)	04. Cumplimiento de leyes y regulaciones externas	05. Transparencia financiera	06. Cultura de servicio orientada al cliente	07. Continuidad y disponibilidad del servicio de negocio	08. Respuestas ágiles a un entorno de negocio cambiante	09. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación del producto y del negocio
Metas Relacionas con las TI			**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	1	Alineamiento de TI y estrategia de negocio	P	P	S			P	S	P	P	S	P		P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y fiable para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Tabla 19: Relación Metas / Metas Corporativas según objetivo 3

Las Metas de TI seleccionadas para este objetivo son:

La Meta Corporativa número 03: optimización de los costes de los procesos de negocio, se relaciona directamente con:

- ✓ FINANCIERA: meta número 4: riesgos de negocio relacionados con las TI gestionados.
- ✓ FINANCIERA: meta número 10: seguridad de la información, infraestructura de procesamiento y aplicaciones.
- ✓ INTERNA: meta número 16: personal del negocio y de las TI competente y motivado.

La Meta Corporativa número 20: cumplimiento con las políticas internas, se relaciona directamente con:

- ✓ FINANCIERA: meta número 2: cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
- ✓ INTERNA: meta número 10: seguridad de la información, infraestructura de procesamiento y aplicaciones.
- ✓ INTERNA: meta número 15: cumplimiento de las políticas internas por parte de las TI.

- **Identificación de los procesos**

Teniendo ya las metas de TI, se procede a identificar los procesos que aportan más a la realización del objetivo, de la misma forma que se utilizó para el mapeo de metas TI se procede para los procesos teniendo en cuenta entre primarios y secundarios como se ve en (Anexo: L)

Para el Objetivo 1. Con las dos metas de TI identificadas: *8: Uso adecuado de aplicaciones, información y soluciones de tecnología, 16: Personal de negocio y de las TI competente y motivado*, se realiza el mapeo, ilustración 18 y de identificar los Procesos ver tabla 21.

			Metas Relacionadas con las TI																	
			1 Alineamiento de TI y estrategia de negocio	2 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4 Riesgos de negocio relacionados con las TI gestionados	5 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6 Transparencia de los costes, beneficios y riesgos de las TI	7 Entrega de servicios de TI de acuerdo a los requisitos del negocio	8 Uso adecuado de aplicaciones, información y soluciones tecnológicas	9 Agilidad de las TI	10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.	11 Optimización de activos, recursos y capacidades de las TI	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro presupuesto y satisfaciendo los requisitos y normas de calidad.	14 Disponibilidad de información útil y fiable para la toma de decisiones	15 Cumplimiento de las políticas internas por parte de las TI	16 Personal del negocio y de las TI competente y motivado	17 Conocimiento, experiencia e iniciativas para la innovación de negocio
Procesos de Cobit 5			Financiera						Cliente		Interna								Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S				P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S			S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S			S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S						P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P					S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S							
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P			S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S			S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S			
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P				
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P				S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S				S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P				S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P					P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S	S	S	P	S	S	S			S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S				S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P				S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P				P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P				S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S					S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S			P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S			P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S			S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S			S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P			S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S					S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S						S		S

Tabla 20: Identificación de Procesos, según objetivo 1

Para el Objetivo 2. Con las metas de TI identificadas: *2.Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas, 5.Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI, 6.Transparencia de los costes, beneficios y riesgos de las TI, 10.Seguridad de la información, infraestructura de procesamiento y aplicaciones, 11.Optimización de activos, recursos y capacidades de las TI y 15.Cumplimiento de las políticas internas por parte de las TI*. Se realiza el mapeo, ver ilustración 19 y se identificar los Procesos ver tabla 21

			Metas Relacionadas con las TI																
			1 Alineamiento de TI y estrategia de negocio	2 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4 Riesgos de negocio relacionados con las TI gestionados	5 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6 Transparencia de los costes, beneficios y riesgos de las TI	7 Entrega de servicios de TI de acuerdo a los requisitos del negocio	8 Uso adecuado de aplicaciones, información y soluciones tecnológicas	9 Agilidad de las TI	10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.	11 Optimización de activos, recursos y capacidades de las TI	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro presupuesto y satisfaciendo los requisitos y normas de calidad.	14 Disponibilidad de información útil y fiable para la toma de decisiones	15 Cumplimiento de las políticas internas por parte de las TI	16 Personal del negocio y de las TI competente y motivado	17 Conocimiento, experiencia e iniciativas para la innovación de negocio
Procesos de Cobit 5			**Financiera**						**Cliente**		**Interna**								**Aprendizaje y Crecimiento**
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S					P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Manage Human ResourcesGestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S	S	S	P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S					S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Tabla 21: Identificación de procesos, según objetivo 2

Para el Objetivo 3. Con las metas de TI identificadas: *2.Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas, 4.Riesgos de negocio relacionados con las TI gestionados, 10.Seguridad de la información, infraestructura de procesamiento y aplicaciones, 15.Cumplimiento de las políticas internas por parte de las TI y 16.Personal del negocio y de las TI competente y motivado*. Se realiza el mapeo, ver ilustración 20 y se identificar los Procesos ver tabla 22.

			Metas Relacionadas con las TI																	
			Alineamiento de TI y estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Procesos de Cobit 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S					P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Manage Human ResourcesGestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S	S		S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S	S	S	P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Tabla 22: Identificación de procesos, según objetivo 3

Resumen total de los procesos escogidos de acuerdo a las metas empresariales y TI, por cada uno de los objetivos tabla 23.

Metas Empresariales	Metas TI	Procesos
Objetivo 1		
14.Productividad operacional y de los empleados	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas	APO04 BAI05 BAI07
16.Personas preparadas y motivadas	16.Personal del negocio y de las TI competente y motivado	EDM04 APO01 APO07
Objetivo 2		
12.Optimización de los costes de los procesos de negocio	5.Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	EDM02 APO04 APO05 APO06 APO11 BAI01
	6. Transparencia de los costes, beneficios y riesgos de las TI	EDM02 EDM03 EDM05 APO06 APO12 APO13 BAI09
	11.Optimización de activos, recursos y capacidades de las TI	EDM04 APO01 APO03 APO04 APO07 BAI04 BAI09 BAI10 DSS01 DSS03 MEA01
15.Cumplimiento con las políticas internas	2.Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	APO01 APO12 APO13 BAI10 DSS05 MEA01 MEA02 MEA03
	10.Seguridad de la información, infraestructura de procesamiento y aplicaciones	EDM03 APO12 APO13 BAI06 DSS05
	15.Cumplimiento de las políticas internas por parte de las TI	EDM03 APO01 MEA01 MEA02

Objetivo 3		
3.Riesgos de negocio gestionados (salvaguarda de activos)	4.Riesgos de negocio relacionados con las TI gestionados	EDM03 APO10 APO12 APO13 BAI01 BAI06 DSS01 DSS02 DSS03 DSS04 DSS05 DSS06 MEA01 MEA02 MEA03
	10.Seguridad de la información, infraestructura de procesamiento y aplicaciones	EDM03 APO12 APO13 BAI06 DSS05
	16. Personal del negocio y de las TI competente y motivado	EDM04 APO01 APO07
15.Cumplimiento con las políticas internas	2.Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	APO01 APO12 APO13 BAI10 DSS05 MEA01 MEA02 MEA03
	10.Seguridad de la información, infraestructura de procesamiento y aplicaciones	EDM03 APO12 APO13 BAI06 DSS05
	15.Cumplimiento de las políticas internas por parte de las TI	EDM03 APO01 MEA01 MEA02

Tabla 23: Procesos escogidos de acuerdo a los objetivos.

Procesos escogidos por priorización

Se debe priorizar y escoger los procesos que contribuyan y ayuden directamente a la realización necesaria de los objetivos teniendo en cuenta las actividades, entradas y salidas de cada uno de estos y como están relacionados con las metas TI siguiendo lo establecido en Cobit 5 catalizadores y Cobit 5 para riesgos, este análisis va enfocado en gestionar el riesgo, que es el objetivo de esta tesis, teniendo en cuenta esto los procesos escogidos son:

Procesos de Cobit 5		
Evaluar, Orientar y Supervisar	EDM02	Asegurar la Entrega de Beneficios
	EDM03	Asegurar la Optimización del Riesgo
	EDM04	Asegurar la Optimización de los Recursos
	EDM05	Asegurar la Transparencia hacia las partes interesadas
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI
	APO03	Gestionar la Arquitectura Empresarial
	APO04	Gestionar la Innovación
	APO05	Gestionar el portafolio
	APO06	Gestionar el Presupuesto y los Costes
	APO07	Gestionar los Recursos Humanos
	APO10	Gestionar los Proveedores
	APO11	Gestionar la Calidad
	APO12	Gestionar el Riesgo
	APO13	Gestionar la Seguridad
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos
	BAI04	Gestionar la Disponibilidad y la Capacidad
	BAI05	Gestionar la introducción de Cambios Organizativos
	BAI06	Gestionar los Cambios
	BAI07	Gestionar la Aceptación del Cambio y de la Transición
	BAI08	Gestionar el Conocimiento
	BAI09	Gestionar los Activos
	BAI10	Gestionar la Configuración
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio
	DSS03	Gestionar los Problemas
	DSS04	Gestionar la Continuidad
	DSS05	Gestionar los Servicios de Seguridad
	DSS06	Gestionar los Controles de los Procesos del Negocio
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Tabla 24: Procesos escogidos por priorización

Los procesos EDM (Evaluar, Orientar y Sustentar), no serán tenidos en cuenta ya que están dirigidos únicamente al gobierno y es responsabilidad del consejo superior como se explicó en su adaptación, para establecer una metodología de gestión de riesgo las actividades y procesos escogidos tendrán alta significancia, teniendo en cuenta el proceso APO12 como prioridad ya que establece seis fases: Recopilación de Datos, Análisis del Riesgo, Mantener un Perfil del Riesgo, Expresar el Riesgo, Definición de un Portafolio de Acciones y Respuesta al Riesgo que plantea el desarrollo desde su planeación, ejecución y evaluación de las actividades que permiten el tratamiento de riesgo.

Teniendo en cuenta la metas corporativas y las metas TI se hizo un análisis de las practicas según Cobit 5 catalizadores y Cobit 5 para riesgos tomando las actividades que más aportan en nuestro análisis, según los objetivos planteados, y como mediante estas se pueda cumplir las metas corporativas como la cascada de Cobit 5 nos demuestra, los riegos que se presentan en las actividades de cada uno de los procesos escogidos, son un análisis que ayuda a entender a nivelo global sobre el ámbito de los riesgos que se deben tener en consideración.

Ejemplo:

La actividad "*06.Gestionar el personal contratado"* del proceso "*APO07 Gestionar los Recursos humanos"*, identifica un riesgo posible que se puede materializar si la entidad no contrata el personal adecuado con las capacidades requeridas necesarias según la tarea a realizar, o asigne roles sin tener en cuenta estas capacidades. Podemos ver como se identifica un posible riesgo en esta actividad si no es tenida en cuenta. De la misma forma a través del cumplimiento y buen desarrollo de esta actividad la entidad puede evitar que el riesgo se genere.

Como se evidencia en la tabla 26 se establecen las actividades más importantes de cada uno de los objetivos. A través de este análisis se logra la primera fase: Recopilación de Datos y se logra entender generalmente como se puede establecer e identificar donde están los posibles riesgos, con esta información se da paso a la obtención de los escenarios de riesgo.

				Mejorar y mantener las habilidades del personal de tal forma que su cocimiento vaya enfocado en el desempeño de actividades relacionadas con las Tecnologías de la Información.	Mejorar la infraestructura de TI disponible mediante la optimización de costos que permitan invertir en medidas de seguridad para de esta forma conseguir los diferentes objetivos y metas planteadas en la entidad	Identificar, analizar, evaluar y reducir los riesgos en la entidad a través de la implementación de un sistema de seguridad de la información que cumpla las políticas internas.
				Objetivo1	**Ojetivo2**	**Objetivo3**
Dimencion	**Id**	**Proceso**	**Actividades**			
Alinerar, Planificar y Organizar	APO06	Gestionar el Presupuesto y los Costes	**.01 Gestionar las finanzas y la contabilidad**			
			.02 Priorizar la asignación de recursos			
			.03 Crear y mantener presupuestos.			
			.04 Modelar y asignar costes.			
			.05 Gestionar costes.			
	APO07	Gestionar los Recursos Humanos	**.01 Mantener la dotación de personal suficiente y adecuada.**			
			.02 Identificar personal clave de TI.			
			.03 Mantener las habilidades y competencias del personal.			
			.04 Evaluar el desempeño laboral de los empleados.			
			.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.			
			.06 Gestionar el personal contratado.			
	APO12	Gestionar el Riesgo	**.01 Recopilar datos.**			
			.02 Analizar el riesgo.			
			.03 Mantener un perfil de riesgo.			
			.04 Expresar el riesgo			
			.05 Definir un portafolio de acciones para la gestión de riesgos.			
			.06 Responder al riesgo.			
	APO13	Gestionar la Seguridad	**.01 Establecer y mantener un SGSI**			
			.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.			
			.03 Supervisar y revisar el SGSI.			
Construccion, Adquisicion e Implementacion	BAI06	Gestionar los Cambios	**.01 Evaluar, priorizar y autorizar peticiones de cambio.**			
			.02 Gestionar cambios de emergencia.			
			.03 Hacer seguimiento e informar de cambios de estado.			
			.04 Cerrar y documentar los cambios.			
	BAI09	Gestionar los Activos	**.01 Identificar y registrar activos actuales**			
			.02 Gestionar activos críticos			
			.03 Gestionar el ciclo de vida de los activos			
			.04 Optimizar el coste de los activos.			
			.05 Administrar licencias.			
Entregar, dar Servicio y Soporte	DSS05	Gestionar los Servicios de Seguridad	**.01 Proteger contra software malicioso (malware).**			
			.02 Gestionar la seguridad de la red y las conexiones.			
			.03 Gestionar la seguridad de los puestos de usuario final.			
			.04 Gestionar la identidad del usuario y el acceso lógico.			
			.05 Gestionar el acceso físico a los activos de TI.			
			.06 Gestionar documentos sensibles y dispositivos de salida.			
			.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.			
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	**.01 Establecer un enfoque de la supervisión.**			
			.02 Establecer los objetivos de cumplimiento y rendimiento			
			.03 Recopilar y procesar los datos de cumplimiento y endimiento.			
			.04 Analizar e informar sobre el rendimiento.			
			.05 Asegurar la implantación de medidas correctivas.			
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	**.01 Supervisar el control interno.**			
			.02 Revisar la efectividad de los controles sobre los procesos de negocio.			
			.03 Realizar autoevaluaciones de control.			
			.04 Identificar y comunicar las deficiencias de control.			
			.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.			
			.06 Planificar iniciativas de aseguramiento.			
			.07 Estudiar las iniciativas de aseguramiento.			
			.08 Ejecutar las iniciativas de aseguramiento			
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	**.01 Identificar requisitos externos de cumplimiento.**			
			.02 Optimizar la respuesta a requisitos externos.			
			.03 Confirmar el cumplimiento de requisitos externos.			
			.04 Obtener garantía de cumplimiento de requisitos externos			

Tabla 25: Actividades Importantes

5.4.2. Análisis de Riesgo

5.4.2.1. Elección de Escenarios de Riesgos para TI

De acuerdo con el procedimiento planteado en la adaptación, en esta parte se deben identificar los escenarios propuestos por Cobit 5 para riesgos que se deben aplicar al proyecto, para la ayuda en la identificación de dichos escenarios se tuvo en cuenta los objetivos creados, las actividades y prácticas correspondientes a cada uno de los procesos priorizados de acuerdo a la tabla 25, y también junto con las encuestas (Anexo: J) que generaron riesgos como podemos ver en la tabla 6 más acordes a la realidad de la entidad de manera que en conjunto se obtenga un resultado más completo.

La formulación de los escenarios de riesgos se basa en la estructura de los escenarios de riesgos proporcionados por COBIT 5 para Riesgos, el cual presenta veinte situaciones en las cuales una entidad en general puede sufrir pérdidas, sin embargo, estos riesgos deben ser comparados con la entidad de manera que el resultado sea objetivo y pertinente.

Teniendo en cuenta las actividades que se escogieron tabla 26, los escenarios genéricos de Cobit 5, los riesgos encontrados mediante las encuestas, la ubicación de la entidad, la recolección de información, en conjunto se utilizara para identificar los escenarios de riesgos con la mayor exactitud que corresponda a nuestro caso.

Para el desarrollo del presente trabajo se han considerado seguir los tres pasos mencionados del flujo de trabajo en el desarrollo de escenarios de riesgo explicados en la fase 2 de la adaptación de Cobit 5.

Ejemplo 1 Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad):

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Tipo de Riesgo			Escenarios Negativos
			Habilitación de beneficio/valor para TI	Entrega de programas y proyectos de TI	Entrega de operaciones y servicios de TI	
25	0804	Infraestructura (hardware, sistemas operativos y tecnologías de control)	P	S	P	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).

Tabla 26: Ejemplo de escenario 1

La relación con el servicio de energía, comunicaciones con el área es muy importante ya que es indispensable para su funcionamiento, el área funciona está dividida en dos partes, la oficina que es donde el personal mediante una computadora recolecta, tramita y envía la información, tanto fuera de la Universidad como a sus dependencias, y donde se alojan los servidores y las aplicaciones que dan funcionamiento a todo el sistema de la Universidad.

El riesgo a un apagón en las oficinas de recaudos es muy alto ya que no cuenta con plantas de energía que solvente este problema, mientras se soluciona este, en cuanto a los servidores, si tiene un reabastecimiento de energía que puede durar hasta un día sin el servicio.

Ahora la comunicaciones entre estas dos dependencia es sin duda importante, porque el soporte del sistema está alojado en el servidor que se encuentra a unos 700 metros de donde se ubica la oficina, se ha tenido en ocasiones pasadas total falta de conexión por robo y saboteo de cableado que une estas dos instalaciones, dejando completamente inservible la Facturación de la Universidad.

Para el tipo de riesgo se han considerado como Primario a dos de ellos: Habilitación de valor y Operaciones de Servicios de TI entregados pues el riesgo afecta la operatividad de la entidad y genera destrucción del valor por la ausencia o ineficiencia del control.

Ejemplo 2 Existen dificultades operativas cuando se pone un nuevo software en producción:

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Tipo de Riesgo			Escenarios Negativos
			Habilitación de beneficio/valor para TI	Entrega de programas y proyectos de TI	Entrega de operaciones y servicios de TI	
65	0904	Software	P		S	Existen dificultades operativas cuando se pone un nuevo software en producción.

Tabla 27: Ejemplo de escenario 2

A través de experiencias pasadas y la falta de políticas de TI así como las habilidades en TI de los empleados no son actualizadas ni se someten a una evaluación periódica, en el momento de introducir un nuevo software repercute en problemas de manejo del

mismo, en conflictos con procedimientos anteriores y en demoras en el servicio, así como la posible pérdida de información.

Para estas eventualidades el personal debe estar lo suficientemente capacitado para una reacción que permita el libre funcionamiento del sistema, esto se consigue solo si se tiene pleno conocimiento de las capacidades del personal actual y si se encuentra actualizado ante las nuevas tecnologías.

Los riesgos que esto puede conllevar se traducen en perdida de información, demoras en el servicio, o total ausencia de servicio.

Por lo mencionado anteriormente se considera el riesgo como Primario en lo referente a la habilitación de valor pues la efectividad de un proceso que se basa en el uso de la tecnología se ve comprometida por no estar actualizadas las habilidades del personal y sus correspondientes políticas.

Ejemplo 3 No es posible acceder a las instalaciones y edificios debido a una huelga gremial:

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Tipo de Riesgo			Escenarios Negativos
			Habilitación de beneficio/valor para TI	Entrega de programas y proyectos de TI	Entrega de operaciones y servicios de TI	
98	1701	Acción industrial	S	S	P	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.

Tabla 28: Ejemplo de escenario 3

Un problema común en este país son las posible huelgas tanto del mismo personal, como de otros ajenos a las instalaciones, como es paro de trasportadores, estudiantiles, indígenas, campesinos, etcétera. En este ámbito la universidad no está exenta de estos inconvenientes ya que son a menudo hechos que se han vuelvo de nuestro diario vivir y que conllevan posibles riesgos que es la ausencia parcial o total del personal a cargo de manejo del sistemas, muchos de estos funcionarios no pueden ser remplazados temporalmente.

Para este riesgo se ha evaluado que de los tres tipos de riesgos, afecta a Operaciones de Servicios de TI Entregados considerado como Primario, esto porque la falta de atención a aquellas partes implica un determinado nivel de problemas respecto del funcionamiento del sistema o programa relacionado con TI.

Ejemplo 4 Hay un terremoto:

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Tipo de Riesgo			Escenarios Negativos
			Habilitación de beneficio/valor para TI	Entrega de programas y proyectos de TI	Entrega de operaciones y servicios de TI	
103	1901	Actos de la Naturaleza	S	S	P	Hay un terremoto.

Tabla 29: Ejemplo de escenario 4

Al centrarnos en riesgos totalmente ajenos a las capacidades actuales del hombre en predecir y evitar un acontecimiento de esta magnitud, y aunque eventos como estos son de muy baja frecuencia en termino del historia, sin embargo el ultimo terremoto de alta intensidad que se efectuó en la ciudad de Popayán fue en el año 1983 que se categorizo como una catástrofe en la ciudad y produjo daños irreversibles siendo recordado como un evento de gran pérdida que afecto las estructuras gravemente.

Es un riesgo presente y que aunque no evitable se puede con la tecnología actual tratar de mitigar los efectos, daños estructurales y pérdida de información, adecuando las instalaciones y protegiendo debidamente los servidores y equipos necesarios, pues un evento de estos afectaría directamente el soporte físico del área de recaudos dejándola inservible, o sacándola de funcionamiento por un tiempo indeterminado.

Para este riesgo se ha evaluado que de los tres tipos de riesgos afecta la Entrega de Operaciones y Servicios de TI, considerándolo como Primario, esto porque la falta de atención a aquellas partes implica un determinado nivel de problemas respecto al servicio que presta el área de Recaudos.
Con las entrevistas realizadas y la información recolectada se procedió a crear nuevos escenarios de riesgos que se pueden dar en la entidad, de acuerdo a los requerimientos y guías que Cobit 5 para riesgos brinda.

Con los escenarios de Riesgos Genéricos de TI sugeridos por el Modelo COBIT 5, se escogieron 55 escenarios, y de acuerdo a la información obtenida mediante esta investigación se generó 10 nuevos escenarios, en total son 65 escenarios obtenidos (ver anexo M)
Escenarios Genéricos escogidos:

			Tipo de Riesgo			
No	**Ref de COBIT 5**	**Categoría de escenario de Riesgo**	**Habilitación de beneficio/valor para TI**	**Entrega de programas y proyectos de TI**	**Entrega de operaciones y servicios de TI**	**Escenarios Negativos**
1	301	Toma de decisiones sobre inversiones en TI	P		S	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (p.ej. nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).
2	401	Pericia y Habilidades TI	P	P	P	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.
3	408		S	P	P	Existe una dependencia excesiva del personal clave de TI.
4	409		S	P	P	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.
5	502	Operaciones del personal (error humano e interno malicioso)	S		P	El equipo de TI es dañado accidentalmente por el personal.
6	503		S		P	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)
7	504		S		P	La información es ingresada incorrectamente por el personal.
8	505		S		P	El centro de datos es destruido (por sabotaje, etc.) por el personal.
9	506		S		P	Un dispositivo con datos sensibles es robado por un miembro del personal.
10	507		S		P	Un componente clave de la infraestructura es robado por un miembro del personal.
11	509		S		P	Se configuran erróneamente los componentes de hardware.
12	510		S		P	El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)
13	601	Información (brecha de datos: daño, fuga y acceso)	S		P	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.
14	602		S	S	P	La base de datos está corrupta, lo cual hace inaccesible a los datos.
15	603		S	S	P	Perdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)
16	604		S	S	P	Se pierden y se revelan datos sensibles mediante ataques lógicos.
17	605		S	S	P	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.
18	606		P	S	P	Se revela información sensible en forma accidental debido a fallas en el seguimiento de

						las guías de manejo de información.
19	607		P	S	P	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)
20	608		P	S	P	Se revela información sensible a través del correo electrónico.
21	609		P	S	P	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.
22	801	Infraestructura (hardware, sistemas operativos y tecnologías de control)	P	S	P	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.
23	802		P	S	P	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.
24	803		P	S	P	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.
25	804		P	S	P	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).
26	806				P	Fallas en el hardware por exceso de calor.
27	901	Software	P		S	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).
28	902		P		S	Se implementa software inmaduro (adopción temprana, fallos, etc.)
29	903		P		S	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.
30	904		P		S	Existen dificultades operativas cuando se pone un nuevo software en producción.
31	905		P		S	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.
32	906		P		S	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.
33	907		P		S	Modificación no intencional del software conduce a resultados inesperados.
34	908		P		S	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.
35	909		P		S	Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.
36	910		P		S	Pocas veces, ocurren problemas con el software de sistemas importantes.
37	1105	Selección / desempeño del proveedor, cumplimiento contractual, discontinuidad del servicio y trasferencia.		S	P	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)
38	1106			S	P	Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.
39	1201	Cumplimiento	P	S	S	No se cumple con regulaciones, que tienen

		regulatorio				que ver con la privacidad, contabilidad, manufactura, etc.
40	1202		P	S	S	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo
41	1401	Robo o destrucción de la infraestructura	S	S	P	Se ha producido el robo de un dispositivo con datos sensibles.
42	1403		S	S	P	Se destruye el centro de datos (sabotaje, etc.).
43	1404		S	S	P	Dispositivos individuales se destruyen accidentalmente.
44	1501	Código Maliciosos	S		P	Se ha producido una intrusión de código malicioso en los servidores operativos.
45	1502		S		P	Los computadores portátiles se infectan frecuentemente con código malicioso.
46	1503		S		P	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.
47	1504		S		P	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.
48	1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.
49	1605		S		P	Existen ataques de virus.
50	1701	Acción industrial	S	S	P	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.
51	1702		S	S	P	El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).
52	1801	Ambiental	S	S	P	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)
53	1901	Actos de la Naturaleza	S	S	P	Hay un terremoto.
54	1903		S	S	P	Hay fuertes tormentas y ciclones tropicales.
55	1904		S	S	P	Hay un gran incendio fuera de control.

Tabla 30: Elección de escenarios de riesgo.

La tabla 31, muestra los escenarios genéricos seleccionados, analizados y establecidos por COBIT 5 para Riesgos. Los escenarios creados por la lista de riesgos según la información obtenida son:

			Tipo de Riesgo			
No	**Ref de COBIT 5**	**Categoría de escenario de Riesgo**	**Habilitación de beneficio/valor para TI**	**Entrega de programas y proyectos de TI**	**Entrega de operaciones y servicios de TI**	**Escenarios Negativos**
56	105	Establecimiento y mantenimiento del portafolio.	P	S	S	Desconocimiento de las Políticas de TI
57	207	Gestión del ciclo de vida del programa o proyecto	P	S	S	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.
58	410	Pericia y Habilidades TI	P		P	Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI.
59	411		P	S	S	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.
60	612	Información (Brecha de datos: daños fugas y accesos)			P	Filtración de la información debido al abandono del equipo de la institución.
61	613		S	S	P	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.
62	807	Infraestructura (hardware, sistema operativo y la tecnología de control) (selección / implementación, operación y desmantelamiento)	S	S	P	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.
63	1405	Robo o destrucción de Infraestructura	P	S	P	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.
64	1406				P	Libre acceso a las instalaciones de procesamiento sin peticiones formales.
65	1505	Códigos maliciosos	P	S	P	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.

Tabla 31: Nuevos escenarios de riesgo

5.4.2.2. Determinación de los Escenarios de Riesgos

Teniendo seleccionados los Escenarios de Riesgos, se procede a su evaluación, la cual se hace considerando calificaciones al probable impacto de ocurrencia en caso de que el riesgo se materialice; y la frecuencia con la posibilidad de ocurrencia del riesgo.

Cabe mencionar que el riesgo es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos, este se mide a través de la probabilidad de que una amenaza se materialice explotando una vulnerabilidad ocasionando así un impacto.

Los criterios de impacto fueron tomados por trabajos pasados los cuales son soportados por varias tesis elaboradas y aceptadas en el exterior por países que han implementado COBIT 5 en sus empresas u organizaciones y los criterios de frecuencia fueron tomados por, Risk IT [34] está también de la familia de ISACA.

5.4.2.2.1. Definiciones de Niveles de Impacto y Frecuencia

Se establece un análisis de impacto cubriendo cinco tipos generales:

Escala	Criterio
8	Desastroso
5	Mayor
3	Moderado
2	Menor
1	Insignificante

Tabla 32: Niveles de Impacto

Se determina un análisis de frecuencia cubriendo cinco tipos generales, los cuales fueron tomados de Risk IT, de tal manera que ajustándolo al trabajo realizado, se establecido de la siguiente manera, de tal forma que se adapte para la valoración del riesgo:

Escala	Valor	Criterio
5	100	Alto
4	10	Medio
3	1	Bajo
2	0.1	Medio Bajo
1	0.01	Raro
0	0.001	

Tabla 33: Niveles de Frecuencia

El último valor de la escala, “0” no se toma debido a que no existe la posibilidad de que ocurra a niveles tan bajos de frecuencia.

5.4.2.3. Evaluación de los Escenarios de Riesgos de acuerdo al Impacto y Frecuencia

Una vez se identificaron los criterios de Impacto y Frecuencia, y teniendo seleccionados los escenarios de riesgos se procede a calcular el Riesgo.

El cálculo de riesgo se determina mediante la fórmula **Frecuencia * Impacto;** cabe resaltar que los resultados obtenidos no son 100% exactas, si no que se requerirá de la mejor estimación posible.

Ejemplo:

Según los esquemas de calificación que fueron planteados con anterioridad, se obtiene lo siguiente:

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Escenarios Negativos	Impacto	Frecuencia	Riesgo
5	408	Pericia y Habilidades TI	Existe una dependencia excesiva del personal clave de TI.	8	5	40
24	904	Software	Existen dificultades operativas cuando se pone un nuevo software en producción	5	1	5
54	1502	Código Maliciosos	Los computadores portátiles se infectan frecuentemente con código malicioso.	8	2	16

Tabla 34: Ejemplo Cálculo de Frecuencia e Impacto

En la tabla 34, el escenario de riesgo Nº 5 se califica con una probabilidad de impacto desastroso debido a la dependencia tan grande que se identificó en el personal, ya que muchas de las funciones importantes están cubiertas solo por una persona que en su ausencia dejara sin un funcionamiento el área dando como resultado un riesgo inaceptable el cual debe ser tenido en cuenta ya que tiene facilidad de materializarse.

El escenario de riesgo Nº 24 se califica con una probabilidad de impacto mayor, ya que al no manejar adecuadamente nuevo software y tener dificulta en el desarrollo de la funciones de este, se verá reflejado en datos erróneos o servicio lento y tedioso como resultado tenemos un riesgo aceptable, el cual debe ser monitoreado para evitarlo, pero su frecuencia es muy baja y se han tomado las medidas necesarias antes de implementar un nuevo aplicativo, por lo que el personal está debidamente capacitado para cualquier actualización.

El escenario de riesgo Nº 54 se califica con una probabilidad de impacto desastroso debido a que la entidad depende totalmente de un software para su funcionamiento y un virus puede detener el sistema, eliminar datos, robar información, etc. El riesgo es

elevado, aunque la frecuencia es baja y se tiene un buen soporte para contrarrestar cualquier ataque de virus, se debe tener en cuenta ya que un posible ataque dejaría comprometida la información y la disponibilidad del servicio.

Los criterios de evaluación presentados en el anexo (Anexo: N) son únicamente para efectos de esta Tesis por tanto pueden variar al ser aplicados a la realidad algún otro procedimiento de la División de Gestiona Financiera u otra empresa.

5.4.2.4. Mapas de Riesgos – Resultado de la Evaluación

Los Mapas de Riesgo, permiten detectar y evaluar a simple vista si la gestión que ha se venido desarrollando para el tratamiento de los mismos, ya sean: operativos, estratégicos, proyectos; ha sido efectiva, es decir, que los escenarios de riesgos son una herramienta flexible que favorece la adopción de medidas inmediatas considerando todas aquellas personas, áreas, unidades o departamentos que influyen activamente para que dichos riesgos sean contrarrestados de manera óptima.

Este mapa utiliza un grafo de riesgo, el cual se encuentra relacionado con la fórmula establecida anteriormente mencionada, se consideran estos valores de manera que constituyen un tipo de coordenada para ubicar el riesgo en el que se encuentra el área de Recaudos. Tomando estos dos conceptos se forman una matriz de la cual no existe un estándar único que establezca su dimensión, pero se suelen usar de 3x3, 4x4 y 5x5. Para efecto de esta tesis y según los criterios de impacto y frecuencia, se propone una matriz de 5x5.

Riesgo= Frecuencia * Impacto							
Desastroso	**Impacto**	**8**	8	16	24	32	40
Mayor		**5**	5	10	15	20	25
Moderado		**3**	3	6	9	12	15
Menor		**2**	2	4	6	8	10
Insignificante		**1**	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
		Frecuencia					
			Raro	**M. Bajo**	**Bajo**	**Medio**	**Alto**

Tabla 35: Matriz de Riesgo

En base a los al producto de las variables, se obtiene un rango de resultados de los cuales se tienen diferentes grupos de riesgos definidos por las bandas de colores en el mapa de riesgos; los criterios de los colores con sus respectivas definiciones, fueron tomadas por Risk IT; mostrado a continuación:

Riesgo						
				1	2	**Muy Bajo**
		3	4	5	6	**Aceptable**
8	9	10	12	15	16	**Elevado**
15	20	24	25	32	40	**Inaceptable**

Tabla 36: Calificación de Riesgo

- Casillas en rojo o Riesgo Inaceptable: el área de Recaudos estima que este nivel de riesgo es mucho más allá de su apetito de riesgo normal. Cualquier riesgo que se encuentren en esta banda podría desencadenar una respuesta inmediata de riesgos.
- Casillas en amarillo o Riesgo Elevado: el área de Recaudos podría aceptarlo. Requieren mitigación o respuesta adecuada a definir dentro de los límites de tiempo determinado.
- Casillas de color verde o Riesgo Aceptable: normalmente con ninguna acción especial requerida, excepto el mantenimiento de los controles actuales o de otras respuestas.
- Casillas de color azul o Riesgo Muy Bajo: indican que es un riesgo, donde el ahorro del costo de oportunidades se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir.

5.4.2.4.1. Elaboración del Mapa de Riesgo para el área de Recaudos

La elaboración del Mapa de Riesgo del área de Recaudos, se desarrolló de manera que los resultados del Riesgo calculados frente al impacto y la frecuencia de cada uno de los escenarios establecidos del anexo (Anexo: O) se clasifiquen según tipo de riesgo en el que se encuentra, cabe resaltar, dependiendo del valor obtenido, de donde se tiene los siguientes resultados:

Niveles de Riesgo	Referencia de COBIT 5	Respuesta al Riesgo
Inaceptable	105-301-408-409-503-504-506-509-603-604-605-606-607-908-609-612-804-807-1202-1401-1403-1404-1405-1406-1503-1504-1505-1601-1801-1901-1903-1904	Mitigar
Elevado	207-401-502-505-507-601-602-608-613-901-903-907-1105-1201-1501-1502-1702-	Compartir / Transferir
Aceptable	411-412-510-801-802-902-904-906-1106-1605-1701-	Aceptar
Muy Bajo	803-806-905-909-910-	Evitar

Tabla 37: Niveles de Riesgo en Recaudos

5.4.3. Expresar el Riesgo

Los riesgos identificados deben ser dados a conocer a las partes interesadas; una vez analizados los riesgos se obtiene la plantilla en la cual se distingue: el actor, tipo de amenaza, evento, valoración detección y tipo de riesgo; esto servirá para dar a conocer a las partes interesadas internas como por ejemplo, a la alta dirección como el jefe de la División de Gestión Financiera, el jefe de la Vicerrectoría Administrativa, Rectoría y por último al Consejo Superior de la Universidad del Cauca para hacer un respectivo análisis de los riesgos encontrados y hacer su respectivo análisis de respuesta. Cabe mencionar, que los datos referenciados en el anexo (Anexo: P) son tomados de las especificaciones que COBIT 5 para Riesgos da para su valoración.

Ejemplo:

Ref de COBIT 5	Categoría de Escenario de Riesgo	Escenario de Riesgo	Actor		Tipo de Amenaza				Evento							Activo / Recurso				
			Interno	Externo	Maliciosa	Accidental	Error	Falla	Revelación	Interrupción	Modificación	Robo	Destrucción	Reglas y Regulaciones	Ejecución Ineficiva	Personas y habilidades	Estructuras Organizativas	Infraestructuras	Información	Aplicaciones
105	Establecimiento y mantenimiento del portafolio	Desconocimiento de las Políticas de TI.																		
301	Toma de decisiones sobre inversiones en TI	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).																		

Tabla 38: Ejemplo de expresar el riesgo

Para ilustración 38, en el escenario N° 105 pertinente a la categoría del escenarios establecimiento y mantenimiento del portafolio, el riesgo afecta directamente al personal de la entidad por lo que el actor es interno y su origen se centra en un error ya que no se han creado políticas de TI. El evento se relaciona con reglas y regulaciones, podemos ver que es un problema relacionado con la estructura organizativa de la organización.

5.4.4. Definición de un portafolio de acciones para el Riesgo

Con los resultados adquiridos de la valoración de riesgos se debe realizar una serie de análisis, el cual brinde una mejora frente al riesgo. Para la definición de un portafolio de acciones, se seleccionaron los controles y los objetivos de control más adecuados para los riesgos cuyo tratamiento fue el de Mitigar, los cuales fueron identificados en el (Anexo: O)

Para el desarrollo de los controles nos remitimos nuevamente al estándar ISO/IEC 27000, específicamente al estándar ISO/IEC 27002, el cual permite determinar los controles aplicables al área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca; cabe resaltar que únicamente son nombrados mas no ejecutados, esto debido a que su identificación es parte de la fase plan, el cual es el objetivo del trabajo de grado.

La siguiente tabla muestra los controles aplicables al presente trabajo de grado.

Ref. de COBIT 5	Escenarios de Riesgos	Objetivo de Control	Control
105	Desconocimiento de las Políticas de	5. Políticas de la seguridad de la	5.1.1: Políticas para la

	TI.	Información.	seguridad de la información.
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	14. Adquisición, desarrollo y mantenimiento de sistemas	14.2.5: Principios de construcción de los sistemas seguros.
408	Existe una dependencia excesiva del personal clave de TI.	6. Organización de la seguridad de la Información.	6.1.1: Roles y responsabilidades para la seguridad de la información.
		13. Seguridad de las comunicaciones.	13.2.4: Acuerdos de confidencialidad o de no divulgación de información.
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	6. Organización de la seguridad de la Información.	6.1.4: Contactos con grupos de interés especial.
		7. Seguridad de los recursos humanos.	7.2.2: Toma de conciencia, educación y formación en la seguridad de la información
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	6. Organización de la seguridad de la Información.	6.1.3: contacto con las autoridades.
504	La información es ingresada incorrectamente por el personal.	6. Organización de la seguridad de la Información.	6.1.3: contacto con las autoridades.
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	7. Seguridad de los recursos humanos.	7.2.3: Proceso disciplinario.
509	Se configuran erróneamente los componentes de hardware.	11. Seguridad física y del entorno.	11.2.4: Mantenimiento de equipo.
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	9. Control de Acceso.	9.4.5: control de acceso a códigos fuente de programas.
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
		12. Seguridad de las operaciones.	12.1.1: Procedimientos de operación documentada.
			12.3.1: Respaldo de la información.
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	6. Organización de la seguridad de la información.	6.2.1: Políticas para dispositivos móviles.
		8. Gestión de activos.	8.3.1: Gestión de medios removibles.
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	6. Organización de la seguridad de la información.	6.2.2: teletrabajo.
		9. Control de Acceso.	9.4.4: uso de programas utilitarios privilegiados.
609	Se revela información sensible debido a ineficientes procedimiento de retención / archivo y eliminación.	6. Organización de la seguridad de la información.	6.2.1: Políticas para dispositivos móviles.
			6.2.2: Teletrabajo.
		10. Criptografía.	10.1.1: política sobre el uso de

			controles criptográficos.
		11. Seguridad física y del entorno.	11.1.6: Áreas de Despacho y carga
612	Filtración de la información debido al abandono del equipo de la institución.	6. Organización de la seguridad de la información	6.2.2: Teletrabajo.
		9. Control de Acceso.	9.4.3: sistema de gestión de contraseñas.
		11. Seguridad física y del entorno.	11.1.2: Controles de acceso
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	9. Control de Acceso.	9.1.2: Acceso a la redes y a servicios e red.
		11. Seguridad física y del entorno.	11.2.3: seguridad del cableado.
		14. Adquisición, desarrollo, y mantenimiento de sistemas.	14.1.3: protección de transacciones de los servicios de las aplicaciones.
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	9. Control de Acceso.	9.1.1: Política de control de acceso.
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	12. Seguridad de las operaciones.	12.4.1: Registro de eventos.
			12.1.2: Gestión de Cambios
		8. Gestión de activos.	8.3.1: Gestión de medios removibles.
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	14. Adquisición, desarrollo, y mantenimiento de sistemas.	14.2.9: prueba de aceptación de sistemas.
		12. Seguridad de las operaciones.	12.1.2: Gestión de Cambios
1401	Se ha producido el robo de un dispositivo con datos sensibles.	9. Control de Acceso.	9.2.2: Suministro de acceso de usuarios.
		11. Seguridad física y del entorno.	11.1.2: Controles de acceso
			11.2.1: Ubicación y protección de equipos.
1403	Se destruye el centro de datos (sabotaje, etc.).	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de los equipos.
1404	Dispositivos individuales se destruyen accidentalmente.	11. Seguridad física y del entorno.	11.2.2: servicios de suministro.
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	9. Control de Acceso.	9.1.1: Política de control de acceso.
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	12. Seguridad de las operaciones.	12.2.1: controles contra códigos maliciosos.
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	9. Control de Acceso	9.4.4: uso de programas utilitarios privilegiados.
		12. Seguridad de las operaciones.	12.2.1: controles contra códigos maliciosos.
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita	9. Control de Acceso	9.4.1: restricción de acceso a la información.
			9.4.3: Sistemas de gestión de contraseñas.

	el acceso de software.		
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	9. Control de Acceso	9.4.3: Sistemas de gestión de contraseñas.
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	8. Gestión de activos.	8.2.3: Manejo de activos.
1901	Hay un terremoto.	11. Seguridad física y del entorno.	11.1.4: Protección contra amenazas externas y ambientales.
1903	Hay fuertes tormentas y ciclones tropicales.		
1904	Hay un gran incendio fuera de control.		

Tabla 39: Controles a Implementar

De la lista de controles dados por ISO/IEC 27002, existen aquellos que se excluyeron debido a que ya fueron implementados o no presenta ningún riesgo que se pueda mitigar con dicho control. Para ello la tabla 39 identifica los controles que ya han sido implementados dentro del área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca.

Objetivo de Control	Control
6.1: Organización interna: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	6.1.5: Seguridad de la información en la gestión de proyectos: la seguridad de la información se debe tratar en la gestión de proyectos independiente del tipo de proyecto.
7.1: Antes de asumir el empleo: Asegurar que los empleados y los contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	7.1.1: Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	7.1.2: Términos y condiciones de empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información
7.3: Terminación y cambio de empleo	7.3.1: Terminación o cambio responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
8.1: Responsabilidad por los activos: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	8.1.1: Inventario de activos: se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	8.1.2: Propiedad de los activos: los activos mantenidos en el inventario deben tener un propietario.
	8.1.3: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
	8.1.4: Devolución de los activos: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la

	organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
8.2: Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización.	8.2.1: Clasificación de la información: la información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada
8.3: Manejo de medios: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada.	8.3.3: Transferencia de medios físicos: los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
9.2: Gestión de acceso de usuarios. Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	9.2.6: Retiro o ajustes de los derechos de acceso: los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
14.2: Seguridad en los procesos de desarrollo y de soporte: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	14.2.9: Prueba de aceptación de los sistemas: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
16.1: Gestión de Incidentes y mejoras en la seguridad de la información: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunidad sobre eventos de seguridad de debilidades.	16.1.2: Reporte de eventos de seguridad de la información: Los eventos de seguridad de la información se debe informar a través de canales de gestión apropiados, tan pronto como sea posible.
18.1: Cumplimiento de requisitos legales y contractuales. Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación, o contractuales relacionadas con la seguridad de la información y cualquier requisito de seguridad.	18.1.1: identificación de la legislación aplicable y de los requisitos contractuales: todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.

Tabla 40: Controles Implementados

De igual manera la estrategia que da COBIT 5, la cual procede con la identificación de las acciones requeridas para reducir el riesgo Inaceptable; para ello se determinaron actividades de COBIT 5 Procesos Catalizadores para tratar los riesgos [35] y ayudar a Recaudos a cumplir con los objetivos estratégicos de la División de Gestión Financiera.

En el anexo (Anexo: Q), se consideraron los escenarios calificados en nivel de alto riesgo, los cuales tienen la necesidad de describir las actividades que se deben llevar a cabo para tratar los riesgos; los responsables son el personal, quienes ponen en práctica las acciones y se encargan de rendir cuentas por la realización de las mismas; de esta manera se diferencian los responsables que están específicamente relacionados con el área de Recaudos y otros que hacen parte de la División de Gestión Financiera; también se especifican los recursos necesarios para la

implementación y las métricas necesarias para definir la buena efectividad de las actividades; y finalmente se llega a establecer el nivel de Riesgo residual producto de la aplicación de las acciones.

Cabe aclarar que para el análisis de este trabajo se tomaron los controles dados por la ISO /IEC 27002.

5.4.4.1. Riesgo Residual

En el anexo (Anexo: R), se considera la evaluación o definición del nuevo nivel de riesgo de la entidad en relación con los riesgos priorizados a los cuales se hizo su respectivo análisis para poder minimizar el riesgo de alguna manera.

Con la obtención del nivel de riesgo residual se puede realizar una comparación con el nivel de riesgo actual, de manera que se observen los efectos posteriores al decidir implementar las acciones para el tratamiento del riesgo.

Ref de COBIT 5	Escenarios Negativos	Nivel de Riesgo Actual	Riesgo Residual
105	Desconocimiento de las Políticas de TI.	40	6
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	20	10
408	Existe una dependencia excesiva del personal clave de TI.	40	9
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	24	10
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	24	10
504	La información es ingresada incorrectamente por el personal.	32	9
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	24	15
509	Se configuran erróneamente los componentes de hardware.	24	10
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	24	15
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	24	9
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	20	15
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	32	15
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	40	10

609	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.	24	15
612	Filtración de la información debido al abandono del equipo de la institución.	40	15
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	32	9
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	20	15
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	32	8
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	24	6
1401	Se ha producido el robo de un dispositivo con datos sensibles.	32	15
1403	Se destruye el centro de datos (sabotaje, etc.).	40	15
1404	Dispositivos individuales se destruyen accidentalmente.	32	15
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	40	15
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	40	15
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	40	15
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	40	15
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	25	9
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	40	8
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	24	15
1901	Hay un terremoto.	40	15
1903	Hay fuertes tormentas y ciclones tropicales.	40	15
1904	Hay un gran incendio fuera de control.	40	15

Tabla 41: Comparación del Riesgo actual / riesgo residual

5.4.5. Respuesta al Riesgo

Finalmente con el análisis realizado anteriormente sobre la gestión de riesgos se presenta el Plan de Acciones para el Tratamiento de los Riesgos, en el que se sintetizan los riesgos con su respectivo nivel, las actividades, los responsables e indicadores para evaluar la eficiencia de dichas medidas. Adicionalmente se define el nivel de respuesta al riesgo que se va a alcanzar con las acciones propuestas en el caso de ser implementadas.

Ref. de COBIT 5	Escenarios Negativos	Respuesta			
		Mitigar	Compartir / Trasferir	Aceptar	Evitar
105	Desconocimiento de las Políticas de TI.				
207	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.				
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).				
401	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.				
408	Existe una dependencia excesiva del personal clave de TI.				
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.				
411	Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI				
412	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.				
502	El equipo de TI es dañado accidentalmente por el personal.				
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)				
504	La información es ingresada incorrectamente por el personal.				
505	El centro de datos es destruido (por sabotaje, etc.) por el personal.				
506	Un dispositivo con datos sensibles es robado por un miembro del personal.				
507	Un componente clave de la infraestructura es robado por un miembro del personal.				
509	Se configuran erróneamente los componentes de hardware.				
510	El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)				
601	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.				
602	La base de datos está corrupta, lo cual hace inaccesible a los datos.				
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)				

604	Se pierden y se revelan datos sensibles mediante ataques lógicos.				
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.				
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.				
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)				
608	Se revela información sensible a través del correo electrónico.				
609	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.				
612	Filtración de la información debido al abandono del equipo de la institución.				
613	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.				
801	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.				
802	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.				
803	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.				
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).				
806	Fallas en el hardware por exceso de calor.				
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.				
901	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).				
902	Se implementa software inmaduro (adopción temprana, fallos, etc.)				
903	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.				
904	Existen dificultades operativas cuando se pone un nuevo software en producción.				
905	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.				
906	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.				
907	Modificación no intencional del software conduce a resultados inesperados.				
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.				
909	Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.				
910	Ocurren problemas con el software de sistemas importantes.				
1105	Pueden existir incumplimientos de las licencias de				

	software (uso y/o distribución de software sin las correspondientes licencias, etc.)				
1106	Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.				
1201	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.				
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo				
1401	Se ha producido el robo de un dispositivo con datos sensibles.				
1403	Se destruye el centro de datos (sabotaje, etc.).				
1404	Dispositivos individuales se destruyen accidentalmente.				
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.				
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.				
1501	Se ha producido una intrusión de código malicioso en los servidores operativos.				
1502	Los computadores portátiles se infectan frecuentemente con código malicioso.				
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.				
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.				
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.				
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.				
1605	Existen ataques de virus.				
1701	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.				
1702	El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).				
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)				
1901	Hay un terremoto.				
1903	Hay fuertes tormentas y ciclones tropicales.				
1904	Hay un gran incendio fuera de control.				

Tabla 42: Respuesta al Riesgo

6. Descripción de la lista de chequeo ISO/IEC 27003

La tabla 43 brinda una lista de chequeo de las actividades requeridas para establecer e implementar un SGSI, también apoya el seguimiento del proceso para la implementación y establece una correlación de las actividades de implementación.

El anexo (Anexo: S), muestra toda la documentación de salida requerida por la ISO/IEC 27003 establecida en la tabla 43.

FASE DE IMPLEMENTACIÓN ISO/IEC 27003	NRO. DE PASO	ACTIVIDAD, REFERENCIA ISO/IEC 27003	PASO PRE-REQUISITO	DOCUMENTO DE SALIDA
5.Obtener la aprobación de la dirección para la implementación de un SGSI	1	Obtener objetivos del negocio de la organización	Ninguno	Lista de objetivos de negocio de la organización
	2	Lograr la comprensión de los sistemas de gestión existentes	Ninguno	Descripción de sistemas de gestión existentes
	3	5.2 Definir objetivos, necesidades de seguridad de información, requerimientos del negocio para un SGSI	1,2	Resumen de los objetivos, necesidades de seguridad de información y requerimientos de negocio para el SGSI
	4	Obtener las normas reglamentarias, de cumplimiento y de la industria aplicables a la empresa	Ninguno	Resumen de las normas reglamentarias, de cumplimiento y de la industria aplicables a la empresa
	5	5.3 Definir alcance preliminar del SGSI	3,4	Descripción de alcance preliminar del SGSI(5.3.1) Definición de roles y responsabilidades del SGSI (5.3.2)
	6	5.4 Crear el caso de negocio y el plan de proyecto para aprobación de la dirección	5	Caso de negocio y plan de proyecto propuesto
	7	5.5 Obtener aprobación de la dirección y compromiso para iniciar un proyecto para implementar un SGSI	6	Aprobación de la dirección para iniciar un proyecto para implementar un SGSI
6. Definir alcance y política de un SGSI		Definir límites organizacionales	7	• Descripción de límites organizacionales • Funciones y estructura de la organización • Intercambio de información a través de límites • Procesos de negocio y responsabilidad sobre los activos de información dentro y fuera del alcance
	9	6.3 Definir límites de las tecnologías de la información y las comunicaciones	7	• Descripción de los límites de las TIC • Descripción de sistemas de información y redes de telecomunicación describiendo lo comprendido y lo fuera del alcance
	10	6.4 Definir límites físicos	7	• Descripción de límites físicos para el SGSI • Descripción de la organización y sus características geográficas describiendo alcance interno y externo
	11	6.5 Finalizar límites para el alcance del SGSI	8,9,10	Un documento describiendo el alcance y los límites del SGSI
	12	6.6 Desarrollar la política del SGSI	11	Política del SGSI aprobada por la dirección
7 Realizar un análisis de la organización	13	7.2 Definir los requerimientos de seguridad de la información que den soporte al SGSI	12	Lista de las principales funciones, ubicaciones, sistemas de información, redes de comunicación

				Requerimientos de la organización referentes a confidencialidad, disponibilidad e integridad
				Requerimientos de la organización relacionados a requisitos legales y reglamentarios, contractuales y de seguridad de información del negocio
				Lista de vulnerabilidades conocidas de la organización
	14	7.3 Identificar activos dentro del alcance del SGSI	13	Descripción de los principales proceso de la organización
				Identificación de activos de información de los principales procesos de la organización
				Clasificación de proceso/activos críticos
	15	7.4 Generar una evaluación de seguridad de la información	14	• Documento del estado actual de seguridad de la información de la organización y su evaluación incluyendo controles de seguridad existentes.
				• Documento de las deficiencias de la organización evaluadas y valoradas
8. Realizar una evaluación del riesgo y Seleccionar Opciones de Tratamiento del Riesgo	16	8.2 Realizar una evaluación del riesgo	15	• Alcance para la evaluación del riesgo
				• Metodología de evaluación del riesgo aprobada, alineada con el contexto de gestión de riesgos de la organización.
				• Criterio de aceptación del riesgo.
	17	8.3 Seleccionar objetivos de control y controles	16	Evaluación del riesgo de alto nivel documentada
				Identificar la necesidad de una evaluación del riesgo más detallada
				Evaluación de riesgos detallada
				Resultados totales de la evaluación de riesgos
	18	8.4 Obtener aprobación de la dirección para implementar un SGSI	17	Riesgos y las opciones identificadas para el tratamiento del mismo
				Objetivos de control y controles para la reducción de riesgos seleccionados.
	19	Aprobación de la dirección del riesgo residual	18	Aprobación de la dirección documentada del riesgo residual propuesto (debería ser la salida de 8.4)
	20	Autorización de la dirección para implementar y operar el SGSI	19	Autorización de la dirección documentada para implementar y operar SGSI (debería ser la salida de 8.4)
	21	Preparar declaración de aplicabilidad	18	Declaración de aplicabilidad

Tabla 43: Listado de Chequeo según ISO/IEC 27003

7. CONCLUSIONES, TRABAJOS FUTUROS, APORTES Y EXPERIENCIAS.

7.1. CONCLUSIONES.

- Se definieron estrategias de protección y el plan de mitigación de riesgo, a través del proceso AP012 luego de ser adaptado e integrado a la fase plan del SGSI, obtenido una guía de cada práctica del proceso adecuada para el análisis de riesgo en el área de Recaudos.

- En la evaluación de los Riesgos, es importante tener el criterio y la información adecuada para escoger los escenarios genéricos más apropiados y crear nuevos escenarios, por lo que es muy necesario obtener información completa de la entidad, para de esta manera realizar una evaluación exitosa de los factores de riesgo de cada escenario y priorizar los más riesgosos.

- Se desarrolló la fase de plan del SGSI, según la norma ISO/IEC 27001 y se hizo una evaluación de riesgo completa, obtenido un plan de comunicación de riesgo, para así aplicar los controles con los que se calibro y ajusto mecanismos para la valoración de riesgo que mitigaron el riesgo de todos los escenarios considerados “Inaceptables”, mostrando que fueron acertados los controles seleccionados y el plan de tratamiento elegido para el área de Recaudos de la división Financiera de la Universidad del Cauca.

- El marco de referencia COBIT 5 y sus guías, permite el alineamiento con otros estándares y marcos como ITIL, TOGAF y estándares ISO para proporcionar una referencia de buenas prácticas sólidas, mediante su implementación, desde la creación de metas empresariales hasta obtener las actividades de cada proceso logra un desarrollo pleno en el tratamiento del riesgo que se extiende en la entidad gracias a sus cinco principios y siete catalizadores.

7.2. TRABAJOS FUTUROS.

- Terminar con el desarrollo de las siguientes fases del SGSI, ejecutar, verificar y actuar para el área de Recaudos, a partir de los resultados obtenidos en la fase plan.

- Desarrollar la fase plan, utilizando COBIT 5 para el análisis de riesgos en otros procedimientos críticos de la Universidad del Cauca.

- Implementar el Marco de COBIT 5 para riesgos completo en otros procedimientos críticos de la Universidad del Cauca.

7.4. EXPERIENCIAS

- Durante el desarrollo del presente trabajo de grado se logró conocer en una mejor perspectiva a COBIT 5 para Riesgos, la cual es compleja de entender para personas que quieran explorarla, además no se encuentra información en Colombia que permita tener un soporte de ella por lo cual fue necesario acudir a referencias extranjeras para llevar a cabo la ejecución del presente proyecto.
- COBIT 5 es un estándar que provee una extensa base de conocimiento y aprendizaje, de la cual cabe resaltar que no se encuentra toda la documentación necesaria en español por consiguiente la hace un poco más compleja para el personal que no maneje otro idioma.
- Para la realización de las respectivas entrevistas, reuniones con el personal encargado, se requería tener un conocimiento más profundo acerca de la información que se deseaba obtener, debido a que el personal no tenía un conocimiento claro sobre un SSGI.
- Se evidencia que para el desarrollo de este tipo de trabajos se debe cumplir con varios requerimientos establecidos por la entidad con la cual se va a desarrollar, debido a que el manejo de la información suministrada debe ser confidencial por el alto grado de riesgo.

Bibliografía

[1] INTECO "Curso de Gestion de riesgo" Laboratorio Nacional de Calidad de Software.

[2] ISO, Norma técnica Colombiana NTC - ISO/IEC 27001:2013 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS, Bogotá DC: icontec, 2013.

[3] ISACA “COBIT 5 para Riesgos” disponible en: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[4] Ministerio de las TIC "Plan vive Digital" en: http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html

[5] Gobierno de Colombia "Estrategia de Gobierno en línea" en: http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

[6] Ministerio de las TIC "Modelo de Seguridad de la Informacion para la Estrategia de Gobierno en Linea 2.0": Bogota D.C. Diciembre 2011.

[7] "Estándares de Seguridad ISO 27000", WeLiveSecurity.com, 2016. [En línea]. Disponible: http://www.welivesecurity.com/la-es/2014/09/10/estandares-seguridad-iso-27000-nuevo/. [Última Búsqueda: 10- Febrero - 2016].

[8] ISO, GUÍA TÉCNICA COLOMBIANA GTC - ISO/IEC 27003, TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Bogotá DC: Icontec, 2012.

[9] "El Ciclo de Deming", *Implementacionsig.com*, 2016. [En línea]. Disponible: http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-.

[10] "Estandares de Seguridad ISO 27002" [En linea]. Disponible: http://www.iso27000.es/iso27002.html

[11] "Estandares de Seguridad ISO 27004" [En linea]. Disponible: http://www.iso.org/iso/catalogue_detail?csnumber=42106

[12] "ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management", *ISO*, 2011. [En línea]. Disponible: http://www.iso.org/iso/catalogue_detail?csnumber=56742.

[13] "Estandares de Seguridad ISO" [En linea]. Disponible: http://www.iso27000.es/iso27000.html

[14] A. G. Alexander, Diseño de un sistema de gestion de seguridad de informacion, Bogotá, Colombia: Alfa Omega Colombiana S.A., 2007.

[15] "Seguridad de la Informacion en Colombia" [En linea]. Disponible: http://seguridadinformacioncolombia.blogspot.com.co/2010/06/declaracion-de-aplicabilidad-statement.html

[16] "Documento Conpes 3072", Republica de Colombia*, Departamento Nacional de Planeación*, 2000. [En línea]. Disponible: http://www.mintic.gov.co/portal/604/articles-3498_documento.pdf

[17] Ministerio de las TIC "Decreto 127 de 2001" Nivel Nacional: http://www.mintic.gov.co/portal/604/articles-3551_documento.pdf

[18] Ministerio de las TIC " Decreto 3107 de 2003 " Nivel Nacional: http://www.mintic.gov.co/portal/604/w3-article-3599.html

[19] "Manual GEL 3.1 | Ministerio de Ambiente y Desarrollo Sostenible", *Minambiente.gov.co*, 2014. [En línea]. Disponible: https://www.minambiente.gov.co/index.php/normativa/74-tecnologias-de-la-informacion-y-la-comunicacion/tecnologias-de-la-informacion-y-la-comunicacion-articulos/135-plantilla-areas-tecnologias-de-la-informacion-y-la-comunicacion-6#documentos.

[20] Gobierno en linea. Entregables 3,4,5 y 6: Informe Final - Modelo de Seguridad de la Informacion- Sistema SANSI-SGSI- Modelo de seguridad de la informacion para la estrategia de Gobierno en Linea.

[21] Ministerio de las TIC "Ley 1341 de 2009" Nivel Nacional: http://www.mintic.gov.co/portal/604/w3-article-3707.html

[22] Alcaldia de Bogota " Ley 1273 de 2009" Nivel Nacional:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[23] F. Pino, F. García, M. Piattini and H. Oktaba, "A research framework for building SPI proposals in small organizations: the COMPETISOFT experience", *Software Qual J*, 2015.

[24] R. E. Stake, The art of case study research, Thousand Oaks, CA: Sage, 1995.

[25] Universidad del Cauca, LVMEN Programa : http://www.unicauca.edu.co/prlvmen/bienvenidos-la-portada

[26] ISACA "Cobit 5 para Riesgos" Apéndice C pag 205-215.

[27] Chavarro Flores Freddy Alexander & Mora Potosi Luis Javier (2016) "GESTIÓN DEL RIESGO DE SI[1] CON BASE EN LA NORMA ISO/IEC 27005:2011, ADAPTANDO LA METODOLOGÍA NIST SP 800-30". Universidad del Cauca. Popayan. Colombia.

[28] Ministerio de las TIC "Normativa del Gobierno Electronico en Colombia": Bogota D.C. Diciembre 2011.

[29] Ministerio de las TIC "Estrategia de Gobierno en Linea 2012-2015 para el orden Nacional, 2012-2017 para el orden territorial": Bogota D.C.

[30] *"Políticas del sistema de seguridad de la información de la Universidad del Cauca"*, R-785, Universidad del Cauca, 2015.

[31] "Anexo 13: Tabla de Contenido – Fase Plan – Modelo de Seguridad de la Información para la estrategia de Gobierno en Línea 2.0", Ministerio de Tecnología de la Información y las Comunicaciones, 2011. [En línea]. Disponible: http://css.mintic.gov.co/ap/gel4/images/SeguridaddelaInformacion2-0-1_Anexo13_TOC_ModeloEntidad_Plan.pdf.

[32] ICONTEC, Estándar Internacional NTC ISO/IEC 27005:2008 Information technology — Security techniques — information security risk management (second edition)

[33] ISACA COBIT 5 "Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa"; 2012.

[34] ISACA Risk IT Basado en COBIT "Marco de Riesgos de TI" : 2009

[35] ISACA COBIT 5 "Procesos Catalizadores": 2012