Descargado el: 14-11-2026 ISSN 2500-7718

Artículos de Revisión

Desarrollo y Adaptación de COBIT 5 como metodología de gestión de riesgos a la norma ISO/IEC 27001, utilizando el proceso APO12

Development and Adaptation of COBIT 5 as a risk management methodology to ISO / IEC 27001, using the APO12 process

Juan Pablo Mora Palacios[1] Milena Cruces Cerón[1] Siler Amador Donado[1]

[1] Universidad del Cauca, Popayán, Grupo de Tecnologías de la información GTI, Colombia

Cómo citar este artículo:
Mora Palacios, J., Cruces Cerón, M., & Amador Donado, S. (2017). Desarrollo y Adaptación de COBIT 5 como metodología de gestión de riesgos a la norma ISO/IEC 27001, utilizando el proceso APO12. *GestióN Ingenio Y Sociedad, 2*(1), 18-37. Recuperado de http://gis.unicafam.edu.co/index.php/gis/article/view/22

Resumen

En el presente artículo se resaltan los resultados adquiridos por el análisis de la fase plan de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO/IEC 27001, con su respectiva guía de implementación ISO/IEC 27003, frente al desarrollo y la adaptando de COBIT 5 como metodología de riesgos, utilizando el proceso APO12, concretamente en la fase de valoración de riesgos; seguidamente se proponen un modelo para la conformidad de la norma.

Palabras clave: Investigación y política de la comunicación, Confidencialidad de datos,linformación y comunicación

Abstract

In this article the results obtained by the analysis of the plan of a Management System Information Security (ISMS) phase according to the ISO / IEC 27001 are highlighted, with their respective implementation guide ISO / IEC 27003, compared to development and adapting COBIT 5 as the risk methodology, using the APO12 process, particularly in the risk assessment phase; then a model for the conformity of the proposed standard.

Key words: Research and communication policy, Data confidentiality, Information and communication

Aprobado: 2017-03-10 13:28:13

Correspondencia: Juan Pablo Mora Palacios. Universidad del Cauca jpmora@unicauca.edu.co

INTRODUDDIÓN

Hoy en día, a diario nos encontramos amenazados por riesgos que ponen en peligro la integridad de nuestra información y por consiguiente la conformidad de nuestros negocios. Dichos riesgos pueden provenir tanto del interior como del exterior de nuestras empresas. Debido a lo anterior, para poder trabajar en un entorno como este de forma segura, las empresas pueden asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información o también conocido por sus siglas en español SGSI.

Un Sistema de Gestión de Seguridad de la Información (SGSI), es un conjunto de políticas de administración de la información. Implica crear un 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 la información en el interior de nuestra empresa, ante nuestros clientes y ante las distintas partes interesadas en nuestro negocio.

Cabe resaltar que un SGSI debe estar documentado y ser conocido a distintos niveles por todo el personal, y estar incluido en un proceso global que permita la mejora continua.

Con el fin de proporcionar un marco de Gestión de 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 han sido elaboradas conjuntamente por ISO, que es la Organización Internacional de Normalización, y por IEC, que es la Comisión Electrónica Internacional. Ambos están formados por los organismos de normalización más representativos de cada país.

Estas normas permiten de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal.

La norma principal de la serie es la ISO/IEC 27001. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad.

Esta norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los requisitos que permitan evidenciar el buen funcionamiento del sistema; de igual manera específica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización.

Para el desarrollo del SGSI es necesario decidir con que metodología de valoración de riesgos trabajar y teniendo como base la existencia de muchas de ellas, se lleva a la búsqueda de metodologías que permitan el análisis de los riesgos, para el desarrollo de la implementación y ejecución de gestión del riesgo. Es por eso que se decide probar a COBIT 5 para riesgos de ISACA, el cual por medio de un estudio de Jonathan Carrillo llamado “Gestión del Riesgo en las Metodologías de Proyectos de Tecnologías de Información y Comunicaciones” permite concluir que puede ser apta para el desarrollo. Esto debido a que COBIT se centra en el riesgo y proporciona una orientación más detallada y practica a los profesionales del riesgo y otras partes interesadas en cualquier nivel de la empresa.

DESARROLLO

Estructura de la implementación de un SGSI basado en el estándar ISO/IEC 27001

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:

a) Alcance y límites de un SGSI: este debe determinar las partes o procesos de la organización que van a ser incluidos dentro del mismo. La empresa debe determinar cuáles son los procesos críticos para su organización, decidiendo que es lo que se quiere proteger y por donde se debe empezar. Se debe tener definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedaran excluidas.

b) Política de un SGSI: su principal objetivo es recoger las directrices que deben seguir la seguridad de la información de acuerdo con las necesidades de la organización y la legislación vigente.

c) Análisis y evaluación de la 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). 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.

d) Valoración de Riesgo: 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. La norma ISO/IEC 27001 permite determinar la metodología de gestión de riesgos que mejor se ajuste según las características. 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.

e) Tratamiento de riesgo: 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.

f) Declaración de aplicabilidad: 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 en lista en la norma.

II.Guía de gestión de riesgos COBIT 5 para riesgos- Proceso APO12

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.

Valoración de Riesgos: APO12

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.

El proceso de Gestión de Riesgos APO12 de COBIT 5 para Riesgos, por medio de sus fases, permite establecer el análisis de riesgos; el cual establece inicialmente 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.

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.

ADAPTACIÓN 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 que 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 Fase 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 tomara 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 tomara 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 detallaran las etapas Adaptadas de cada una de las practicas del proceso que llamaremos Fases.

Proceso APO 12: PROCESO DE GESTIONAR EL RIESGO.

Las fases para el análisis de riesgo son identificadas en la figura 1 de acuerdo al proceso APO12 y serán detalladas a continuación:

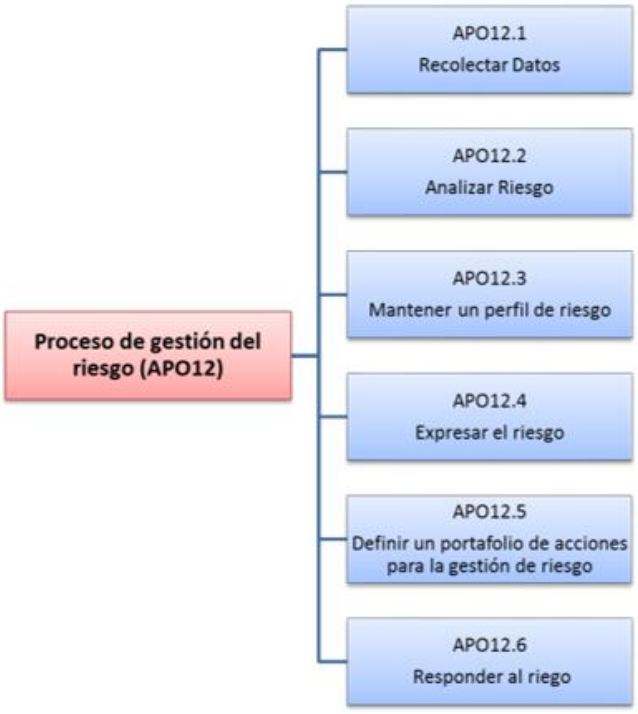


Figura 1: Proceso de Gestión de Riesgo.

1. **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 estas 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.

1. **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 figura 2):

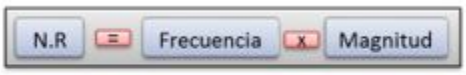


Ilustración 2: Función de riesgo.

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:

1. 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.
2. Escenarios Importantes: Definidos los riesgos que afectan directamente a la consecución de objetivos se debe de priorizar los más riesgosos.
3. Detalle de los riesgos: Mostrar información suficientemente clara que ofrezca 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 11, 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.

1. 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.

1. 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.

1. 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.

1. 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 las siguientes tablas correspondientes a las fases I, II, III; IV, V y VI.

Tabla 1. fase I, recopilar datos.

		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.

Tabla 2. Fase II, analizar riesgo.

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
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 plantillas de Cobit 5 y el análisis de riesgo en la entidad	Se construirán nuevos escenarios solo negativos de acuerdo al caso y se utilizarán 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 ya que no existe una comparación anterior.

Tabla 3. Fase III, mantener un perfil del riesgo.

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
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.

Tabla 4. Fase IV, expresar el riesgo.

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
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 evaluará 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.

Tabla 5. Fase V, definir un portafolio de acciones para la gestión de riesgos.

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
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		

Tabla 6. Fase VI, responder al riesgo.

		Adaptación y Calibración		
Prácticas de gestión	**Actividades para el cumplimiento de la Práctica.**	**Estado**	**Actividades Adaptadas**	**Justificación**
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, 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 adversas pasadas 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		

En la siguiente tabla 7 se observa como algunas Fases del Proceso APO12 de Cobit 5 para riesgos ayudan a alcanzar ciertos requisitos de un SGSI:

Tabla 7: Cumplimiento de requisitos de la norma, aplicando Cobit 5 para riesgos.

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.

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”.

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 8 se muestra la Relación de EPSI de los marcos de referencia

Tabla 8. 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 1 Fase 2 Fase 4
5	Selección de objetivos de control y controles	Fase 5
6	Entregables	Fase 6

Ahora se aplicara el proceso definido en la figura 2 y el resultado está definido en la tabla 8.

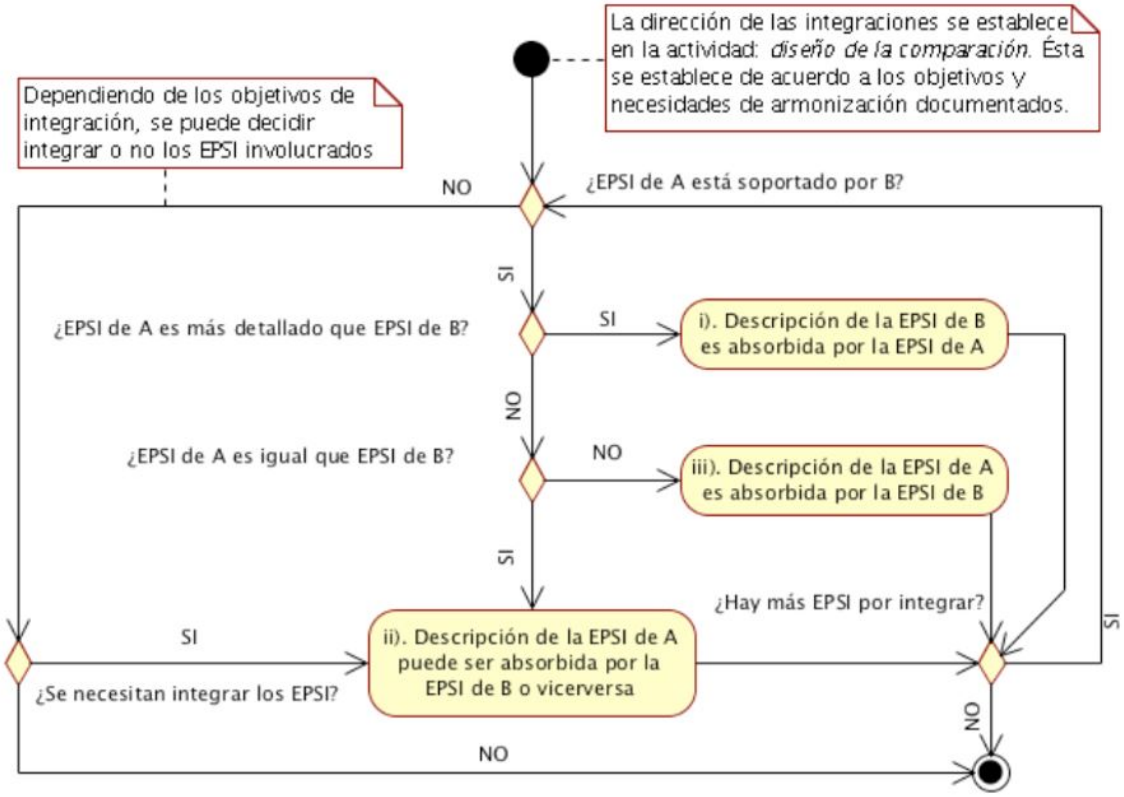


Figura 2: Proceso de comparación e integración

Para definir sin el EP de un marco es más detallado que el EP del otro marco, se usó la siguiente documentación (tabla 9).

- 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

Tabla 9: Integración de marcos de referencia.

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

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

Finalmente se muestra en la Figura 3. 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.

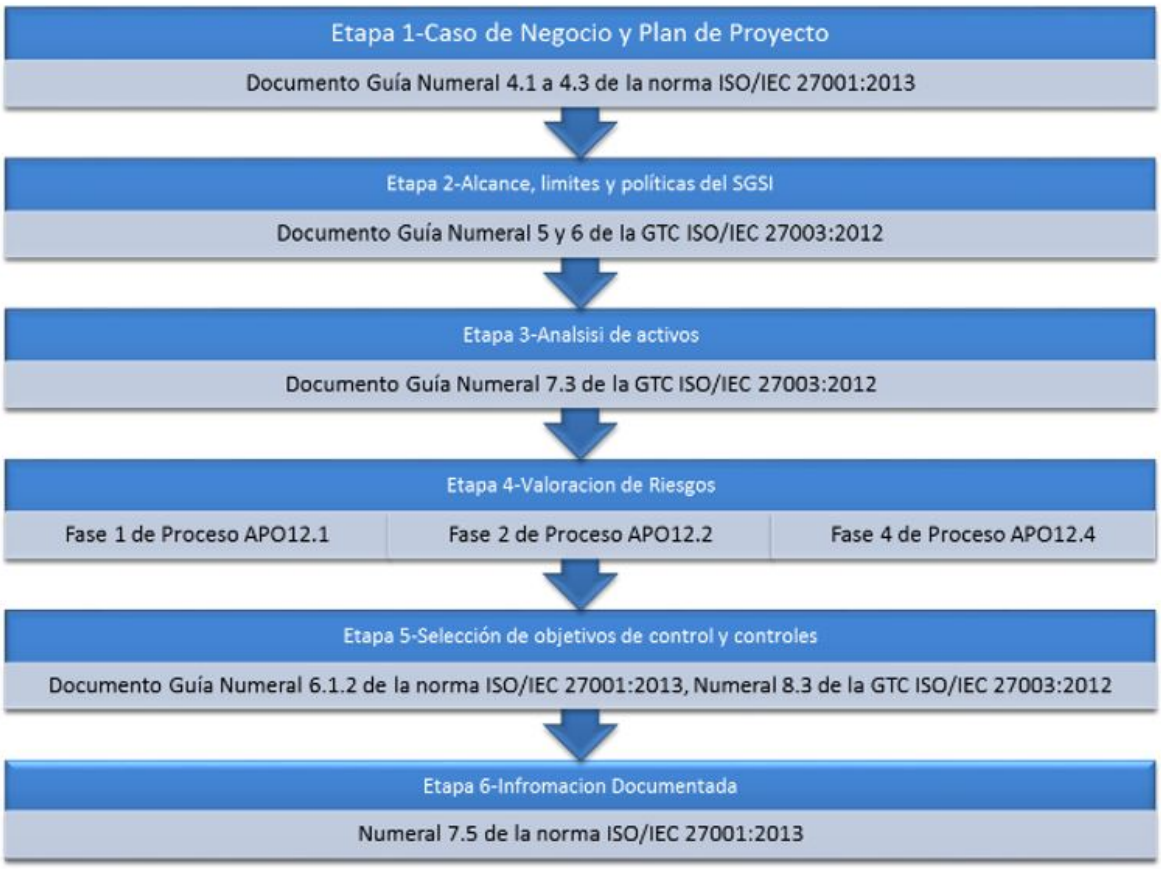


Figura 3: Adaptación de la Metodología de valoración de riesgos.

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.

AGRADECIMIENTOS

Este trabajo ha sido apoyado por la Universidad del Cauca, especialmente por el área de Recaudos de la División de Gestión Financiera y el grupo de Tecnologías de la Información (GTI).

REFERENCIAS BIBLIOGRÁFICAS

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

Cesar Pardo, F. G. (2011). Método de integracion para soportar la armonización de múltiple modelos y estándares. XVI jornadas de ingenieria del software y bases de datos SISTEDES 2011. A Coruña, España.

Gobierno de Colombia. (s.f.). http://estrategia.gobiernoenlinea.gov.co. Recuperado el 13 de 12 de 2015, de http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

ICONTEC. (2013). "Estándar Internacional GTC-ISO/IEC 27003:2012 Information Technology -- security techniques -- Information Security Management System Implementation Guidance".

ICONTEC. (2013). "Estándar Internacional ISO/IEC 27001:2013 Information Technology -- security techniques -- Specification for an information Security Management System.

ICONTEC. (2013). "Estándar Internacional ISO/IEC 27002:2013 Information Technology -- security techniques -- Code of Practice for Information Security Controls".

ICONTEC. (ed, 2011). Estándar Internacional NTC ISO/IEC 27005:2011 Information technology — Security techniques — information security risk management (second edition).

ISO. (2012). 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.

ISO. (2014). ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems - Overview and vocabulary.

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