Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

"Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI"

Trabajo de titulación previo a la obtención del título de:

"Ingeniero en Sistemas y Telemática"

Autor:

Pablo Andrés Minchala Márquez.

Director:

Ing. Paul Esteban Crespo Martínez.

Cuenca, Ecuador

2016

DEDICATORIA

El presente trabajo va dedicado a mis padres y hermano que me guía desde el cielo.

AGRADECIMIENTOS

Quiero agradecer a mi director de trabajo de titulación Ing. Esteban Crespo M, por el apoyo brindado a lo largo del presente trabajo.

ÍNDICE DE CONTENIDOS

DEDICATORIA ii

AGRADECIMIENTOS iii

ÍNDICE DE CONTENIDOS iv

ÍNDICE DE GRAFICOS viii

RESUMEN ix

ABSTRACT x

INTRODUCCIÓN 1

ANTECEDENTES 2

OBJETIVO GENERAL 2

OBJETIVOS ESPECÍFICOS 2

JUSTIFICACIÓN 3

CAPÍTULO I 4

MARCO TEÓRICO 4

1.1 Riesgo 4

1.2 Tratamiento de riesgos 5

1.3 ¿Origen de un riesgo tecnológico? 7

1.4 ¿Qué es un riesgo de información? 10

Actividades estratégicas para evitar Riesgos de Información 11

1.5 ¿Qué es la seguridad de la información? 15

1.6 La Gestión de la Información 15

1.7 ¿Qué es un sistema de gestión de la información? 16

1.8 ¿Un sistema de Gestión de Seguridad de la Información? 17

1.9 ¿Qué son las normas ISO? 21

1.10 Norma ISO 27001 24

1.11 ISO 27002 24

1.12 ISO 27005: LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 27

LOS CUATRO PASOS DE LA IMPLANTACIÓN 27

1.13 ISO 31000 - GESTIÓN DEL RIESGO 28

ISO 31000: 2009 29

1.14 ¿Qué es COSO III? 30

1.15 ¿Qué es COBIT 5? 31

1.16 ¿Qué son las MPYME? 35

CAPÍTULO II 37

2.1 Análisis de la Gestión de Riesgos de TI - COSO III 37

2.1.1 Componente 1 - Entorno de control 37

2.1.2 Evaluación de riesgos 42

2.1.3 Actividades de control 45

2.1.4 Sistemas de información 48

2.1.5 Supervisión del sistema de control - Monitoreo 49

2.2 Proceso de Administración de Riesgos de TI: 51

2.2.1 Establecer Metodología 51

2.2.2 Identificar Riesgos de TI 51

2.2.3 Análisis del Riesgo de TI 51

2.2.4 Evaluación y Priorización de los Riesgos: Método Matricial para el Análisis de Riesgos 53

2.2.5 Diseñar los controles definitivos 54

2.2.6 Presentar los Resultados 55

2.3 COSO III relación con las normas ISO 55

2.4 Conclusión 58

CAPITULO III 61

3.1 Análisis de la Gestión de Riesgos de TI – COBIT 5 61

3.1.1 COBIT 5 para riesgos. 61

3.1.2 Principios de COBIT 5 62

3.1.3 Procesos COBIT 5 para la gestión del riesgo 69

3.2 Riesgo TI. 72

3.2.1 Factores de riesgo interno 73

3.2.2 Gestión de riesgos de TI 73

3.3 COBIT 5 relación con las normas ISO 75

3.4 Conclusión 82

CAPITULO IV 84

4.1 ESTUDIO COMPARATIVO COBIT 5 COSO III..... 84

4.2 Comparación COBIT 5 y COSO III en la gestión de riesgo informático 91

CAPÍTULO V..... 93

CONCLUSIÓNES DE LA INVESTIGACIÓN..... 93

BIBLIOGRAFÍA..... 95

ANEXOS:..... 99

ÍNDICE DE GRAFICOS

GRÁFICO Nº 1: ESQUEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN 17

GRÁFICO Nº 2: ÁREAS CLAVES DE GOBIERNO Y GESTIÓN COBIT 5 34

GRÁFICO Nº 3: VALORAR RIESGO 52

GRÁFICO Nº 4: FÓRMULA PARA CATEGORIZACIÓN DE RIESGO..... 54

GRÁFICO Nº 5: MATRIZ DE RIESGO..... 54

GRÁFICO Nº 6: PRINCIPIOS DE COBIT 5..... 62

GRÁFICO Nº 7: ADAPTABILIDAD DE COBIT 5 A LAS NECESIDADES DE LA EMPRESA MEDIANTE LA CASCADA DE METAS 63

GRÁFICO Nº 8: NECESIDADES DE LAS PARTES INTERESADAS 65

GRÁFICO Nº 9: CATALIZADORES CORPORATIVOS 67

GRÁFICO Nº 10: MODELO DE EVALUACIÓN DE PROCESOS COBIT 5..... 72

GRÁFICO Nº 11: RELACIÓN DE COBIT 5 CON LAS NORMAS ISO..... 75

GRÁFICO Nº 12: RELACIÓN DE COSO III CON LAS NORMAS ISO – PARTE 1 - 2 56

GRÁFICO Nº 13: RELACIÓN DE COSO III CON LAS NORMAS ISO – PARTE 2 - 2 57

GRÁFICO Nº 14: La integración de COBIT 5 y COSO III 84

RESUMEN

La gestión de riesgos es un proceso muy importante en los negocios y organizaciones del siglo XXI. Al encontrarse inmersas en procesos informáticos, se requiere garantizar la disponibilidad, integridad y confidencialidad de la información, que, en la actualidad, es considerada un factor de ventaja competitiva.

Por esta razón, el presente trabajo busca comparar dos metodologías utilizadas en la gestión de riesgos: COBIT 5 y COSO III, validando su cumplimiento con las normativas ISO que son utilizadas para este fin. Sin embargo, por su extensión, muchas veces resultan inalcanzables para las empresas del sector MPYME. Así, como resultado, se concluirá sobre cuál de las metodologías analizadas es la más adecuada para el entorno MPYME ecuatoriano.

ABSTRACT

Risk management is a very important process in the businesses and organizations of the XXI century. Because they are embedded in informatics processes, it is required to guarantee availability, integrity and confidentiality of information, which at present is considered a competitive advantage factor. For this reason, this paper seeks to compare two methodologies used in risk management: COBIT 5 and COSO III; validating their compliance with the ISO standards that are used for this purpose. However, because of their extension, they are often unreachable for companies in the MSME sector. Thus, as a conclusion, this paper will present which of the tested methodologies is best suited for the Ecuadorian MSMEs environment.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

INTRODUCCIÓN

Hoy en día las empresa u organizaciones sin importar su categoría, buscan la competitividad, mediante el fortalecimiento en la gestión de sus procesos administrativos, con el fin de manejar de la forma más eficaz los recursos que posee; alcanzando los objetivos propuestos mediante una toma de decisión acertada, que satisfaga las necesidades de los clientes con los productos o servicios que oferta. Para cumplir con este propósito, hoy por hoy existe una de las áreas más importantes y sensibles en una empresa, la misma que, en el siglo XXI puede llamarse el corazón de la institución; conocida como centro de procesamiento de datos, en donde se gestionan los activos más importantes y delicados de las organizaciones que son los datos e información, los cuales son de muy importantes para la continuidad y alcance de los objetivos institucionales, ya que con ella la empresa tiene mayor ventaja competitiva.

Por estos motivos y con el fin de llevar un mejor control de la información y mitigar las vulnerabilidades que pueden suscitar, desde muchos años atrás existen diferentes metodologías como las normas ISO que continuamente se encuentran desarrollando, mejorando e innovando; permitiendo una mejor gestión de los riesgos. Para el área de tecnologías de la información, por ejemplo, existe la norma ISO 270001; esta normativa proporciona las directrices para establecer un proceso de gestión de seguridad de la información (SGSI), mediante el establecimiento de las mejores prácticas para gestionar, prevenir y mitigar vulnerabilidades internas y externas. Es por ello que la presente investigación tiene como objetivo realizar un estudio comparativo de las metodologías COBIT 5 y COSO III, teniendo en cuenta que estas parten de las normas ISO que generalmente está dividida en múltiples documentos de control, cada uno enfocado a un área o escenario de análisis especifico; por ello se pretende identificar los aspectos más importantes de las ISO 27001, 27002, 27005 y 31000, los cuales han sido considerados al momento de desarrollar las metodologías COBIT 5 y COSO III y finalmente se realizará una comparación de estas dos las metodologías en el ámbito de la gestión de riesgo de información y riesgo informático. Esto permitirá a los lectores inmiscuidos e interesados en el tema, comprender y seleccionar la mejor herramienta para gestionar bien la información que se genera día a día en el mundo empresarial.

CUERPO DEL TRABAJO

ANTECEDENTES

Una metodología nace en función de los requerimientos existentes en un contexto. Así, por ejemplo, COBIT 5, COSO III, entre otras metodologías, parten de requerimientos como son las tecnologías de información, la gestión de riesgo financiero, riesgos de mercado, riesgo operativo, riesgo empresarial, entre otros. Sin embargo, para que estas sean eficientes, deben considerar el marco regulatorio local e internacional, así como las mejores prácticas de la industria que, generalmente, son consolidadas en un documento conocido como ISO.

Las normas ISO generalmente están divididas en múltiples documentos de control, cada uno enfocado a un escenario de análisis o de gestión. De esta manera, el presente documento pretende identificar los aspectos más importantes de las ISO 27001, 27002, 27005 y 31000, los cuales han sido considerados en las prácticas de gestión de riesgo de TI por parte de las metodologías COBIT 5 y COSO III.

OBJETIVO GENERAL

Realizar un análisis comparativo entre las metodologías COBIT 5 Y COSO III utilizadas en el análisis y gestión de riesgo informático.

OBJETIVOS ESPECÍFICOS

- Argumentar teóricamente la gestión de riesgos de información y la gestión de riesgo informático.

- Estudiar la metodología COBIT 5 y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000

- Estudiar la metodología COSO III y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000

- Comparar las metodologías COSO III y COBIT 5 en el ámbito de la gestión de riesgo de información y riesgo informático.

JUSTIFICACIÓN

Actualmente muchas empresas del sector micro, pequeña y mediana (MPYME) no tienen claro el concepto, ni el alcance con el que cuenta la gestión de riesgos, por lo tanto, no adoptan las buenas prácticas para el correcto manejo de esta área integrador, ejecutando mínimos procedimientos de mitigación de riesgo, muchos de ellos, por intuición.

Con este fin, se ha planteado realizar una investigación y evaluación de las normativas existentes en la actualidad y que se puedan aplicar a las MPYME para realizar una correcta y adecuada gestión de riesgos.

CAPÍTULO I

MARCO TEÓRICO

1.1 Riesgo

> Riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro. Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de daño" bajo esas circunstancias. Por ejemplo, desde el punto de vista del riesgo de daños a la integridad física de las personas, cuanto mayor es la velocidad de circulación de un vehículo en carretera mayor es el "riesgo de daño" para sus ocupantes, mientras que cuanto mayor es la imprudencia al conducir mayor es el "peligro de accidente" (y también es mayor el riesgo del daño consecuente). (Rodiguez, 2015)

> La noción de riesgo suele utilizarse como sinónimo de **peligro**. El riesgo, sin embargo, está vinculado a la vulnerabilidad, mientras que el peligro aparece asociado a la factibilidad del perjuicio o daño. Es posible distinguir, por lo tanto, entre riesgo (la **posibilidad de daño**) y peligro (la probabilidad de **accidente** o patología). En otras palabras, el peligro es una causa del riesgo. (Definición.de, s.f.)

Para el investigador riesgo son las posibles fallas o daños que pueden ocurrir durante la ejecución de una actividad ya sea personal o dentro de una organización, la cual se tiene que mitigar, mediante un análisis previo del entorno.

1.2 Tratamiento de riesgos

El tratamiento de riesgo en una institución es primordial, ya que si no se realiza puede estancar la productividad, generando pérdidas económicas y la inestabilidad de la organización.

Al tratar el riesgo como esencial dentro del proceso de auditoría se toman medidas para reducirlo, y también para establecer la forma de soportar las pérdidas que genera. Por lo tanto, existen 6 medidas de tratamiento las cuales 3 son de control del riesgo y las otras 3 de financiación del riesgo. En las primeras 3 podremos encontrar: evitar, prevenir o proteger; y en las segundas están: aceptar, retener o transferir.

El diseño de las medidas de tratamiento puede reflejar la cultura organizacional, la historia de la empresa, la forma en que está organizada y su operación, y el medio en el cual se desempeña.

A continuación, explicaremos cada una de estas:

- EVITAR: Para evitar un riesgo se parte del principio de que su probabilidad es alta y representa un alto peligro para la organización, porque podría traer consecuencias muy graves en caso de la ocurrencia del siniestro, algunas formas de evitar un riesgo es no emprendiendo un nuevo proyecto evaluado como no viable, eliminando la actividad que genera un riesgo o sustituyéndola por otra que no sea tan peligrosa o que no produzca tantas perdidas, como la suspensión de alguna línea de producción, negocio, mercado objetivo, canal de distribución o medio de transporte.

- PREVENIR: Cuando se habla de la medida de prevenir estamos hablando de establecer anticipadamente políticas, normas, controles y procedimientos que lleven a que el evento generador del riesgo no ocurra o disminuya su probabilidad de ocurrencia, existen muchas formas de prevención, pero las más utilizadas son:

  • Inspecciones y pruebas de seguridad.

  • Entrenamiento.

  • Inversión en información.

  • Diversificación.

  • Disminución del nivel de exposición.

  • Mantenimiento preventivo.

  • Medicina preventiva.

- PROTEGER: Al hablar de proteger estamos pensando en medidas que actúan, en el momento de presentarse el riesgo, sobre el recurso amenazado, por ejemplo, los equipos de protección, como los cascos o las gafas, disminuyen el impacto del riesgo de accidente sobre los obreros de una construcción.

  Las medidas de protección de mayor aplicación son:

  • Sistemas automáticos de protección.

  • Equipo de protección personal.

• Plan de emergencia.

• Plan de contingencia.

- ACEPTAR: significa asumir un riesgo y las consecuencias que este atraiga en el momento que se presente. Los riesgos se aceptan cuando la frecuencia es baja e impacto leve, y no pones en peligro la estabilidad de la organización.
- RETENER: Estos se retienen cuando en forma planeada se crea un fondo entre otras cosas para responder ante las posibles pérdidas causadas por su ocurrencia.
- TRANSFERIR: El transferir un riesgo se da cuando se traspasa el riesgo a otra compañía, ya sea por medio de un contrato de outsourcing, o una póliza de seguro. Un modo habitual de transferir el riesgo es cubrirlo mediante un seguro. Esta opción tiene sus ventajas y sus inconvenientes. La ventaja más destacada es que es más sencilla que aplicar y seguramente más económica, ya que nos evitamos la adopción de inversiones, contratación de personal, etc. necesarios si decidiéramos gestionar el riesgo. Por el contrario, la desventaja más clara es que se trata de una medida paliativa, que únicamente se podrá aplicar cuando ya se ha producido el daño y que sólo permitirá recuperar los aspectos económicos.

  La adopción de un seguro forma parte, por lo tanto, de la estrategia de continuidad de negocio. (Mejía, 2008, págs. 36-39)

1.3 ¿Origen de un riesgo tecnológico?

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su

incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad. Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de las vulnerabilidades y los riesgos a los que se exponen las organizaciones. El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar, a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

Medidas de aseguramiento ante el riesgo tecnológico

Hablar de controles y medidas que permitan a las organizaciones contrarrestar este tipo de riesgo puede ser complicado, pero es posible tomar acciones que lleven a su mitigación. El aseguramiento puede realizarse desde los tres niveles antes mencionados. En el nivel físico, las medidas a tomar son de carácter técnico o de seguridad informática, referidas a la aplicación de procedimientos de control y barreras físicas ante amenazas para prevenir daño o acceso no autorizado a recursos e información confidencial que sea guardada en la infraestructura física. Dentro de éstas se encuentran:

- Controles de acceso físico, que pueden incluir el uso de sistemas biométricos y vigilantes para acceso en áreas específicas.
- Manejo de tokens o tarjetas de identificación.
- Controles a nivel de equipos, tales como ubicación y protección, seguridad en cableado o mantenimiento periódico de equipos.

- Servicios básicos (energía, agua y alcantarillado, entre otros) de soporte para continuidad.
- Gestión de medios de almacenamiento removible.
- Controles de vulnerabilidades técnicas, entre otros.

En el nivel lógico, las medidas a tomar se dan con respecto al uso de software y sistemas, enfocadas a proteger los datos y garantizar el acceso autorizado a la información por parte de los usuarios a través de los procedimientos correctos. Como parte de estas medidas se pueden tomar:

- Controles de acceso lógico con la gestión de usuarios, perfiles y privilegios para acceso a aplicaciones y gestión de contraseñas.
- Controles de acceso a la red interna y externa, segregación en redes y controles para asegurar servicios de la red.
- Controles a nivel de teletrabajo y equipos móviles.
- Soluciones de protección contra malware.
- Respaldos de bases de datos e información crítica.
- Protocolos para intercambio de información y cifrado de información.
- Monitoreo de los sistemas, sincronización de relojes y protección sobre registros.
- Limitación en tiempos de conexión a aplicativos y cierres de sesión por inactividad.
- Gestión de control de cambios, entre otros.

El tercer nivel y el más crítico dentro de las organizaciones, dada su naturaleza impredecible, es el personal o recurso humano. Las medidas a este nivel deberían ser más procedimentales, ligadas a la regulación y concienciación. Dentro de éstas se pueden incluir:

- Definición de políticas de seguridad que presenten las correspondientes violaciones con el fin de dar cumplimiento.
- Controles relacionados a acuerdos con terceros, prestación de servicios que se puedan dar con éstos y segregación de funciones.
- Controles a nivel contratación de personal.
- Gestión antes, durante y después de la terminación de los contratos.
- Educación y capacitación continua en aspectos de seguridad.
- Procedimientos e instructivos para manejo de información.
- Políticas de escritorio y pantalla limpia.
- Cumplimiento de legislación aplicable, entre otros. (Ramírez, 2012)

Para el autor los riesgos tecnológicos surgen a medida de los nuevos avances en la informática y porque la información valiosa para las instituciones, es confiada en estas tecnologías. También uno las causas es la deficiencia en el transcurso del desarrollo de software, al no analizar todos los posibles ataques que pueden existir; así como la inadecuada gestión de seguridad.

1.4 ¿Qué es un riesgo de información?

La información es unos de los activos más importantes en la actualidad dentro de una organización y a ves se hace más vulnerable. Las brechas de datos, las ciber amenazas y los fraudes son cada vez más frecuentes. Estas amenazas malintencionadas en combinación con errores humanos destapan puntos débiles en un panorama de información que cambia rápidamente, que cada vez es más complejo y que pone en riesgo la reputación de las marcas. Las empresas luchan por conseguir gestionar sus

archivos en papel, pero con la aparición de los sistemas de información cada vez los datos son confiados y generados por las nuevas tecnologías. Como consecuencia, se enfrentan a unos niveles de riesgo de la información sin precedentes. (Duale, 2013)

El riesgo de la información nos interesa a todos. Así como las empresas protegen los datos de los clientes, empleados y proveedores, muchas también poseen la información personal sobre nosotros como consumidores de sus productos y servicios. Esta información tiene que ser protegida. Para conseguir esto, hay que valorar todas las opciones disponibles para descubrir cómo reducir el riesgo de la mejor manera posible. Cuando se trata de mejores prácticas y de gestionar el riesgo de la información, parece que las empresas podrían aprender mucho las unas de las otras. (Duale, 2013)

Actividades estratégicas para evitar Riesgos de Información

- **Contar con un plan de trabajo.** Menos de la mitad (49%) de las empresas más jóvenes – las que llevan activas entre dos y cinco años – admiten abiertamente que son mucho mejores haciendo cosas que en la planificación estratégica. Las empresas más antiguas, por otro lado – las que llevan operando desde hace más de una década – parece que han aprendido que saber lo que se hace es tan importante como lo que se hace. Así, más de la mitad (56%) tienen una estrategia activa para la monitorización del riesgo, en comparación con solo un 14% de las empresas jóvenes. (Duale, 2013)

- **Establecer parámetros de confidencialidad.** Las empresas más jóvenes son más confiadas a la hora de compartir datos con sus empleados. Únicamente un 18% cree que los empleados son una amenaza para la seguridad de su información y solo la mitad tiene un código de conducta para sus

empleados. Un 42% de las empresas más antiguas ve a sus empleados como una amenaza y dos tercios tienen un código de conducta para el personal. Si la precaución significa la existencia de códigos, directrices y formación para ayudar a los empleados a entender mejor los riesgos y proteger la información, entonces la precaución debería ser fomentada y aplaudida. (Duale, 2013)

- **Analizar los riesgos y amenazas.** Un 66% de las empresas de mayor edad tienen activo un plan de recuperación del negocio, frente a solo un 27% de las empresas más jóvenes. Sin un plan de este tipo, cualquier desastre podría dejar a una empresa inactiva y expuesta a una brecha de datos o pérdida de información de la que nunca se recuperaría. (Duale, 2013)

- **Establecer políticas de revisión y monitoreo continuo.** El estudio revela que las empresas de más antigüedad monitorizan dos veces más que las jóvenes la efectividad de cualquier medida que introducen. No hacer estas pruebas puede conducir a que las empresas más jóvenes desperdicien sus recursos o estén implementando acciones que tengan poco o ningún impacto en la reducción del riesgo. (Duale, 2013)

- **Buscar el auspicio de la alta dirección.** La mitad de las nuevas empresas afirma que su junta directiva no considera el tema de la seguridad de la información como algo muy importante, al contrario que las empresas con más experiencia, que sí prestan atención a este asunto. El respaldo de los

ejecutivos senior es esencial para que el riesgo de la información sea tratado seriamente. (Duale, 2013)

- **Mitigar el riesgo.** A pesar de confiar más en sus empleados, solo algo más de la mitad (52%) de las empresas de nuevo cuño dice que sus empleados *no consideran* la protección de datos como algo relevante. Estas empresas parece que están confiando en personas que podrían no estar excesivamente preocupadas por mantener la información segura. Dos tercios de las empresas maduras dicen que los empleados sí ven la seguridad de la información como un asunto serio. (Duale, 2013)

- **Cambios del contexto.** Las nuevas empresas parecen sentirse más cómodas a la hora de gestionar información estructurada y desestructurada en formato digital o físico en múltiples localizaciones (55% comparado con un 38% de las empresas más antiguas). Este mundo multiformato y multicanal es la nueva realidad. Ya no hay vuelta atrás, así que lo mejor es aceptarlo y adaptarse. (Duale, 2013)

- **La frontera entre lo personal y lo profesional en las redes sociales es difusa y merece la pena tomarse el tiempo para dar los pasos adecuados.** Las fronteras entro lo personal y lo profesional en el uso de las redes sociales aún están delimitándose y representan una pesadilla potencial en términos legales y de protección de datos para aquellas empresas incautas. La confusión general y

la incerteza acerca del uso de las redes sociales se pueden considerar desde una variedad de enfoques y preferencias. Por ejemplo, según nuestro estudio, hemos sabido que más de la mitad (59%) de las empresas más jóvenes controlan el uso que hacen sus empleados de las redes sociales, en comparación con solo un 36% de las empresas más antiguas. Las nuevas empresas prestan mucha atención a Facebook (73%), mientras que las más antiguas prefieren monitorizar la actividad en LinkedIn (67%). Sin embargo, este patrón se invierte a la hora de captar talento: un tercio (31%) de las empresas más antiguas revisan candidatos en Facebook en comparación con solo un 10% de las empresas jóvenes; y un 82% de las empresas jóvenes revisan candidatos en LinkedIn, en comparación con solo un 46% de las empresas más longevas. Si la información que obtienen unos y otros es realmente útil, es algo que no queda muy claro. (Duale, 2013)

- **Buscar el financiamiento.** Todas las compañías coinciden en el que el impacto de una brecha de datos afectaría a la fidelidad del cliente (58%, los dos tipos de empresa) y a la reputación de la marca (52% también ambas). (Duale, 2013)

- **Considerar el elevado costo financiero.** Solo el 3% de las empresas más jóvenes coincide firmemente en que es más importante recortar costes que reducir el riesgo, comparado con un 28% de las empresas más antiguas que comparten esa opinión. (Duale, 2013)

1.5 ¿Qué es la seguridad de la información?

> La Seguridad de la Información posee como objetivo principal la protección de la información y sus sistemas de información sean estos de acceso, uso, divulgación, interrupción o distribución no autorizada. (Asociacion Española para la Calidad, 2016)

> Seguridad es un concepto asociado a la certeza, minimización de riesgos pos planes de contingencia creados. Se puede concebir como seguridad un estado de cualquier sistema sea o no informático, nos indica que dicho sistema o información está libre de peligro, daño o riesgo. (Asociacion Española para la Calidad, 2016)

Para el autor la seguridad de la información nace con el propósito de proteger la información, mediante la protección del acceso a los datos solo a los usuarios indicados, esto a través de los sistemas de la información, también previene el uso malintencionado, divulgación, interrupción o destrucción no autorizada.

Así mismo se debe tener en cuenta que la seguridad total al 100% no es posible, ya que el riesgo siempre es impredecible y está presente en todo momento, ya sea por fallas humanas o fallas del sistema como tal.

1.6 La Gestión de la Información

La información es uno de los activos más importantes en el mundo actual dentro de cualquier organización, y esta debe ser gestionada de manera correcta a través de las tecnologías actuales, como los sistemas de información, los mismo que permiten guardar la información y permiten el acceso a los datos requeridos en el momento deseado por un determinado usuario.

> “la gestión de información es todo lo que tiene que ver con obtener la información correcta, en la forma adecuada, para la persona indicada, al costo correcto, en el momento oportuno, en el lugar indicado para tomar la acción precisa” (Woodman, s.f.).

> La gestión de la información también se refiere a “la coordinación eficiente y eficaz de la información procedente de fuentes internas y externas” (White, s.f.).

"La Gestión de la información (GI) es la denominación convencional de un conjunto de procesos por los cuales se controla el ciclo de vida de la información, desde su obtención (por creación o captura), hasta su disposición final (su archivo o eliminación). Tales procesos también comprenden la extracción, combinación, depuración y distribución de la información a los interesados. El objetivo de la gestión de la información es garantizar la integridad, disponibilidad y confidencialidad de la información" (Barrios, s.f.)

1.7 ¿Qué es un sistema de gestión de la información?

Algunos autores conceptualizan los sistemas de gestión de información como un: "sistema integrado y automatizado para proveer la información que sostenga las funciones de operatividad, gestión y toma de decisiones en una organización" (Davis & Olsón, s.f.).

También, Moreiro González (1998) lo define como: "el conjunto de políticas y normas relacionadas entre sí que se establecen para el acceso y tratamiento de los recursos de información, incluye los registros administrativos y los archivos, el soporte tecnológico de los recursos y el público a que se destina. En su evolución el sistema puede manejar la función de inteligencia corporativa y generar productos de inteligencia" (González, 1998).

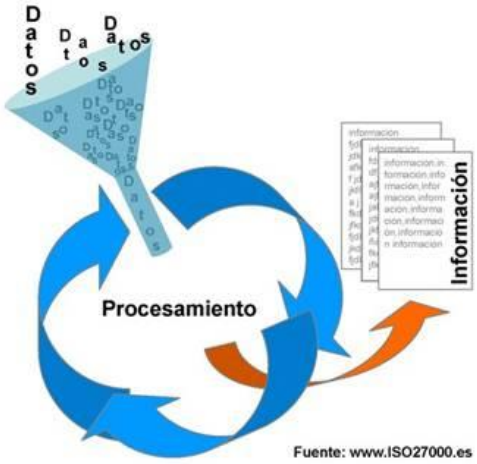
"Cada vez más, las actividades comerciales se desempeñan por medio de redes informáticas. Los sucesos que afectan la integridad de la información pueden afectar la capacidad de la empresa para continuar sus actividades. Las organizaciones deben contar con procesos y procedimientos implantados tanto para asegurar que la información esté protegida como para demostrar su responsabilidad ante las agencias reguladoras y el público" (ABS Quality Evaluations, s.f.).

Para el autor un sistema de gestión de información son un conjunto de tecnologías que permiten el acceso a los datos solo a los usuarios indicados; asegurando a consistencia, integridad y disponibilidad de los datos en el momento requerido; su objetivo es procurar que los usuarios estén satisfechos con los servicios o productos que ofrece la empresa. También ayudan a la toma de decisiones a nivel gerencial, estratégica y operativa.

1.8 ¿Un sistema de Gestión de Seguridad de la Información?

"El SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System" (ISO 27001 en Español, 2016).

GRÁFICO Nº 1: ESQUEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN



Fuente: http://www.iso27000.es/sgsi.html

"En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración" (ISO 27001 en Español, 2016).

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. Este proceso es el que constituye un SGSI, que

podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En la siguiente sección, se desarrollarán los fundamentales de un SGSI según la norma ISO 27001.

Fundamentos:

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D (ISO 27001 en Español, 2016):

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. (ISO 27001 en Español, 2016)

PDCA O Círculo de Deming.

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico, para llevar organizado todo el proceso. El modelo PDCA (Plan, Do, Check, Act), en su equivalencia en español es Planificar, Hacer, Verificar y Actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua. (Universidad Abierta a Distancia UNAD - Colombia, 2016)

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso.

La ISO/IEC 27001 por lo tanto incorpora el típico ***Plan-Do-Check-Act*** (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un enfoque de mejora continua (Universidad Abierta a Distancia UNAD - Colombia, 2016):

- **Plan** *(planificar)*: es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la empresa respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 17799:2005, la cual se pretende implantar para evaluación y certificación.

Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la empresa para el inicio, proceso y ejecución

- Fase de análisis de información de la organización, En esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la empresa para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar.
- **Do** *(hacer)*: es una fase que envuelve la implantación y operación de los controles

En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de empresa. También se formula y se implementa un plan de riesgo

- **Check** *(controlar)*: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizan exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos aceptables y residuales y se realicen periódicamente auditorías internas para el SGSI.

- **Act** *(actuar)*: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante.

Según lo anterior par el autor, los sistemas de gestión de la seguridad de la información (SGSI) surgen junto con el desarrollo de las normas ISO/IEC 27001 e ISO/IEC 27002, donde

manifiesta que este tipo de sistemas tiene el objetivo de brindar la calidad en cuanto a la seguridad de la información, garantizando un nivel de protección aceptable ya que un nivel total es casi imposible, por muchos factores como de disponer un presupuesto limitado, mala administración por parte del personal encargado, persona malintencionadas que buscan la infiltración a los datos con el fin de apropiarse o simplemente hacer un mal a la institución; por tales motivos el fin que persiguen los sistemas de gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, tratados, gestionados y mitigados por la organización de una forma, sistemática, estructurada, repetible, eficiente, escrita o documentada y estos sean adaptables a los cambios que se produzcan el entorno y las tecnologías.

1.9 ¿Qué son las normas ISO?

La organización internacional de estandarización nace con el propósito de realizar nomas o guías en las cuales las diferentes organizaciones pueden sustentarse, para llevar sus procesos de manera estructurada y sistemática; aumentando la productividad y alcance de los objetivos propuestos de manera oportuna, mediante la satisfacción de los clientes con productos o servicios de primera.

> La ISO (*International Standarization Organization*) es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo. Su cede se encuentra situada en Ginebra, es una federación de organismos nacionales entre los que se incluyen AENOR en España, DIN en Alemania, AFNOR en Francia... Entre las normas ISO más utilizadas se encuentran las referentes a las medidas de papel (ISO 216, que contempla los tamaños DIN-A4, DIN-A3, etc.), los nombres de lenguas (ISO 639), los sistemas de calidad (ISO 9000, 9001 y 9004), de gestión medioambiental (ISO 14000), ISO/IEC 80000 para signos y símbolos matemáticos y magnitudes del sistema internacional de unidades, etcétera. Otras curiosas son la ISO 5775 para marcar los neumáticos y las llantas de bicicleta, ISO 9660 para sistemas de

archivos de CD-ROM e ISO 7810 para definir el estándar internacional de las tarjetas de identificación electrónica tipo Visa.

Es una federación mundial de organismos nacionales de normalización (Organismos miembros de ISO). El trabajo de preparación de las normas internacionales normalmente se realiza a través de comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho a estar representado en dicho comité. Las organizaciones internacionales, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (CEI) en todas las materias de normalización electrotécnica. (Posada Moreno, 2007)

Las normas internacionales son editadas de acuerdo con las reglas establecidas en la parte 3 de las Directivas/ISO/CEI.

Los proyectos finales de Normas Internacionales (FDIS) adoptados por los comités técnicos son enviados a los miembros para votación. La publicación como Norma Internacional requiere la aprobación por al menos el 75% de los organismos miembros requeridos a votar. (Posada Moreno, 2007)

A continuación, una reseña breve de lo que significa el Control Total de la Calidad "CTC", haciendo una comparación de la aplicación porcentual de los diferentes ítems que la componen.

- **Control de la Calidad**, lo hacen el 98% de las Empresas.
- **Aseguramiento de la calidad**, lo hacen el 1% de la Empresas.
- **Gestión de la Calidad**, lo hacen el 0,5% de las empresas.
- **Sistemas de Alto Rendimiento**, lo hacen el 0,4% de las empresas
- **Calidad Total Gerencial (TQM)**, lo hacen el 0,1% de las empresas. (Posada Moreno, 2007)

Ahora bien, la Norma NTC ISO 9001:2000 está enfocada a la Gestión de la calidad, en cuyo enfoque podemos advertir que es muy pequeño en número de empresas que se han

comprometido con ella, pero que de alguna manera sus principios y directrices llevan a las empresas a obtener resultados en los siguientes campos:

a) Pone orden en la casa, haciéndola más organizada.

b) Se acoge al Know How de la empresa, se tiene por escrito y no en la memoria de funcionarios o en agendas o papelitos.

c) Atendemos quejas.

d) Buscamos que nuestros clientes no se pierdan, sino que permanezcan en nuestras listas.

e) Administramos más por indicadores, que en forma caprichosa.

f) Las Mejoras y las Acciones Preventivas nos llevan a mejorar nuestra empresa en cuanto a sus productos y servicios.

g) Las acciones correctivas nos presentan ante nuestros clientes como proveedores más amables y competitivos.

h) Existe un desarrollo profesional dentro de nuestros funcionarios, por el entrenamiento.

i) Nos volvemos más disciplinados. Empezamos a dejar aquello de que Dejemos para mañana lo que podemos hacer hoy.

j) Empezamos a hacer énfasis en el orden, el aseo y la seguridad, beneficiándonos todos.

k) Quizás muchos otros que se nos escapan.

Si usted no está obteniendo estos beneficios de su Sistema de Gestión de la Calidad Certificado, permítame decirle que se encuentra desenfocado, si lo aborrece en vez de amarlo, usted se encuentra en el lugar equivocado en cuanto a la administración de la empresa. Cambie su paradigma y verá un mundo maravilloso. (Posada Moreno, 2007)

1.10 Norma ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (ISO 27001 en Español, 2016)

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (27001 Academy, s.f.)

1.11 ISO 27002

Esta norma como muchas otras nace con el fin de mejorar las buenas practicas ya establecidas en normas anteriores, y este es el caso de la norma ISO 27002 que fue publicada como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que la norma ISO 27001 y la ISO 27002 son documentos que están destinados a ser utilizados de forma complementaria. (Gutiérrez, 2013)

ISO / IEC 27002 es un popular estándar internacionalmente reconocido de buenas prácticas para la seguridad de la información. ISO / IEC 27002 remonta su historia de más de 30 años a los precursores de la BS 7799. Para terminar con la revisión de los cambios en la norma para gestionar la seguridad de la información, ISO 27000:2013,

para contar con detalle las novedades sobre la ISO/IEC 27002:2013, la cual está asociada con el Anexo A de la ISO/IEC 27001:2013. (ISO 27002.es, 2016)

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de diciembre de 2009. (ISO 27002.es, 2016)

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria. (ISO 27002.es, 2016)

Dentro de ISO/IEC 27002 se extiende la información de los renovados anexos de ISO/IEC 27001-2013, donde básicamente se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001. En esta nueva versión de la norma se encuentran los controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización. (Gutiérrez, 2013)

Actualización de la norma ISO / IEC 27002: 2013

Con la actualización de esta norma, las organizaciones tienen a disposición un documento que sirve de guía para la implementación de controles para la gestión de la seguridad de la información en una organización, así como de las prácticas más eficaces para gestionarla. Aunque antes de pensar en cómo migrar al nuevo estándar ISO/IEC

27001:2013, es importante tener en cuenta que las categorías de los controles se han mezclado un poco, esto buscando que los dominios de control tengan una estructura más coherente.

Dentro de los cambios interesantes, se debe resaltar que lo relacionado con dispositivos móviles y teletrabajo que antes estaba asociado al "control de accesos", ahora se encuentra dentro de la sección 6: "Organización de la Seguridad de la Información". Y, dentro de la sección de Control de Accesos, se engloba lo relacionado con acceso al sistema operativo, a las aplicaciones y la información. En cuanto a Criptografía, es un dominio de control nuevo: "sección 10", dentro de la cual se incluyen todos los controles criptográficos sugeridos para una organización. En el caso de los controles que deben considerarse cuando se requiera la recuperación de desastres, se encuentran dentro de la sección 17.

Además, cabe resaltar que existen versiones específicas de la norma ISO/IEC 27002, enfocadas en diferentes tipos de empresas: manufactureras, sector de la salud, sector financiero, entre otros. Si bien la nomenclatura ISO es diferente, son normas que toman como referencia la ya mencionada ISO 27002, y por tanto lo tanto están alienados para la correcta gestión de la seguridad de la información.

Es importante recordar la importancia de conocer los cambios sobre los estándares, si bien no influyen sobre la efectividad de la gestión de la seguridad de la información, si ayudan a incrementar su eficiencia, además de ser necesarios para cumplir con todos los requerimientos de una certificación. (Gutiérrez, 2013)

1.12 ISO 27005: LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001. (ISO Tools exelence, 2015)

Se trata de una norma aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización y sustituye a las la normas ISO / IEC TR 13335-3:1998 e ISO / IEC TR 13335-4:2000 de Gestión de la Información y Comunicaciones Tecnología de Seguridad.

El aumento en el uso de tecnologías de la información puede posibilitar brechas o fisuras en aspectos de seguridad con respecto a su utilización, por ello se hace necesaria una gestión de la información desde una perspectiva tecnológica a tres niveles: aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica. (ISO Tools exelence, 2015)

LOS CUATRO PASOS DE LA IMPLANTACIÓN

Basándose en el modelo anterior, una forma de implantar con éxito un Sistema de Gestión de Seguridad de la Información consiste en establecer una hoja de ruta basada en cuatro pasos:

1) Establecimiento de plan de comunicación interno y externo

El plan de comunicación se debe realizar a nivel interno (áreas de la organización, empleados, directivos, socios) y externo (clientes, proveedores, entes reguladores),

teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el informe de los avances del proceso y todo aquello que se considere necesario. Los medios a usar para comunicar el proceso de gestión dependen de las necesidades y disponibilidad de la organización.

2) Definición del contexto organizacional

El objetivo de esta etapa es conocer a la organización para determinar qué puede afectarla a nivel interno y externo, qué elementos se requieren proteger y, de acuerdo a los recursos actuales, cómo podría darse esa protección hasta establecer un nivel de riesgo aceptable.

3) Valoración de los riesgos tecnológicos

En la etapa de valoración de riesgos se identifican los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestos. En este punto se recomiendan posibles controles de mitigación de los riesgos.

4) Tratamiento de riegos tecnológicos

En la etapa de tratamiento de riesgos se establece e implementan las acciones a llevar a cabo para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización. Dentro de las acciones a tomar encontramos principalmente: reducir, aceptar, eliminar y transferir. (ISO Tools exelence, 2015)

1.13 ISO 31000 - GESTIÓN DEL RIESGO

Los riesgos que afectan a las organizaciones pueden tener consecuencias en términos de rendimiento económico y reputación profesional, así como del medio ambiente, la seguridad y los resultados de la sociedad. Por lo tanto, la gestión del riesgo efectivamente ayuda a las organizaciones a realizar bien en un ambiente lleno de incertidumbre. (ISO, 2016)

El estándar ISO 31000 es un marco que le ayuda a examinar, controlar y mejorar continuamente el SGR de una organización. ISO 31000: 2009 proporciona principios y directrices genéricas sobre gestión de riesgos. (ISO, 2016)

La norma ISO 31000 puede ser integrada en otros estándares. Las normas sobre Gestión del riesgo en normas codificadas por la organización International Organization for Standarization. El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo. (ISO, 2016)

Sin embargo, la ISO 31000 no puede ser utilizada para fines de certificación, pero proporciona orientación para la auditoría interna o externa programas. Las organizaciones que utilizan se pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido a nivel internacional, proporcionando sólidos principios para una gestión eficaz y el gobierno corporativo (ISO, 2016)

ISO 31000: 2009

ISO 31000: 2009, Gestión de riesgos - Principios y directrices, ofrece principios, marco y un proceso para la gestión del riesgo. Puede ser utilizado por cualquier organización independientemente de su tamaño, actividad o sector. El uso de ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de que el logro de objetivos, mejorar la identificación de oportunidades y amenazas y efectivamente asignan y utilizan los recursos para el tratamiento del riesgo. (ISO, 2016)

ISO 31000: 2009 puede ser utilizado por cualquier, empresa privada o de la comunidad, asociación, grupo o individuo. Por lo tanto, la norma ISO 31000: 2009 no es específica a cualquier industria o sector. (ISO, 2016)

ISO 31000: 2009 se puede aplicar a lo largo de la vida de una organización, y para una amplia gama de actividades, incluidas las estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos. (ISO, 2016)

ISO 31000: 2009 se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, tanto si tiene consecuencias positivas o negativas.

> Aunque la norma ISO 31000: 2009 proporciona directrices genéricas, no es la intención de promover la uniformidad de la gestión de riesgos en todas las organizaciones. El diseño e implementación de planes de gestión del riesgo y los marcos tendrán que tomar en cuenta las diversas necesidades de una organización específica, sus objetivos particulares, el contexto, la estructura, operaciones, procesos, funciones, proyectos, productos, servicios o activos y prácticas específicas empleadas. (ISO, 2016)
>
> Se pretende que la norma ISO 31000: 2009 se utilizará para armonizar los procesos de gestión de riesgos en las normas existentes y futuras. Proporciona un enfoque común en apoyo de las normas de control de riesgos y / o sectores específicos, y no sustituye a esas normas. (ISO, 2016)

Algo que se debe tener en cuenta es que la norma ISO 31000: 2009 no está previsto para fines de certificación.

1.14 ¿Qué es COSO III?

Committee of Sponsoring Organizations of the Treadway Commission o Comité de Organizaciones Patrocinadoras de la Comisión *Treadway*, es una iniciativa conjunta de cinco organizaciones del sector privado de Estados Unidos, que se dedican a proporcionar liderazgo a través de la elaboración de marcos y orientación sobre la correcta gestión del riesgo empresarial (ERM), el control interno y evitar el fraude.

Las organizaciones que la conforman son:

- La Asociación Americana de Contabilidad (AAA)
- El Instituto Americano de Contadores Públicos Certificados (AICPA) Ejecutivos de Finanzas Internacional (FEI), el Instituto de Auditores Internos (IIA).

- La Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [AMI]).

COSO estudia los factores que pueden generar información fraudulenta dentro de las organizaciones, elabora textos y recomendaciones para ser utilizados por todo tipo de organizaciones y entidades reguladoras. Se lo encuentra como modelo COSO; en cuanto a la gestión de riesgos existen los informes COSO I y II y en mayo del 2013 se publicó la tercera versión COSO III, siendo esta ultima la versión a analizar.

Las novedades que introduce este Marco Integrado de Gestión de Riesgos son:

- Mejora de la agilidad de los sistemas de gestión de riesgos para adaptarse a los entornos.

- Mayor confianza en la eliminación de riesgos y consecución de objetivos.

- Mayor claridad en cuanto a la información y comunicación. (Asociación Española para la Calidad, 2013)

1.15 ¿Qué es COBIT 5?

COBIT 5 – una nueva versión del ya conocido estándar para el cumplimiento de objetivos de control para el CIO (Chief Information Officer - Oficial en Jefatura de Sistemas) y su área. Esta versión, profundamente revisada y mejorada, provee un **marco de referencia integral** que contribuye en la organización al logro de los objetivos y entrega de valor a través de un efectivo gobierno y gestión de la TI empresarial. A partir de su participación en la crítica objetiva en los borradores preliminares del modelo, en este artículo, Sergio Sperat, socio de Estratega y **profesional certificado en el gobierno**

de TI empresarial (CGEIT), responde las preguntas que puede realizar el CIO al integrarse a este nuevo estándar, con el fin de ayudar a descubrir cómo le puede mejorar su gestión.

Entre las preguntas más frecuentes que puede el Oficial de Jefatura de Sistemas son las siguientes:

¿Cuál es el propósito de COBIT?

COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos.

¿Quién utiliza COBIT?

COBIT es empleado en todo el mundo por quienes tienen como responsabilidad primaria los procesos de negocio y la tecnología, aquellos de quien depende la tecnología y la información confiable, y los que proveen calidad, confiabilidad y control de TI. COBIT 5 se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro.

¿Cuáles son los 5 principios de COBIT 5?

- Satisfacer las necesidades del accionista
- Considerar la empresa de punta a punta
- Aplicar un único modelo de referencia integrado

- Posibilitar un enfoque holístico
- Separar gobierno de la gestión.

¿Cuáles son los 7 habilitadores de COBIT 5?

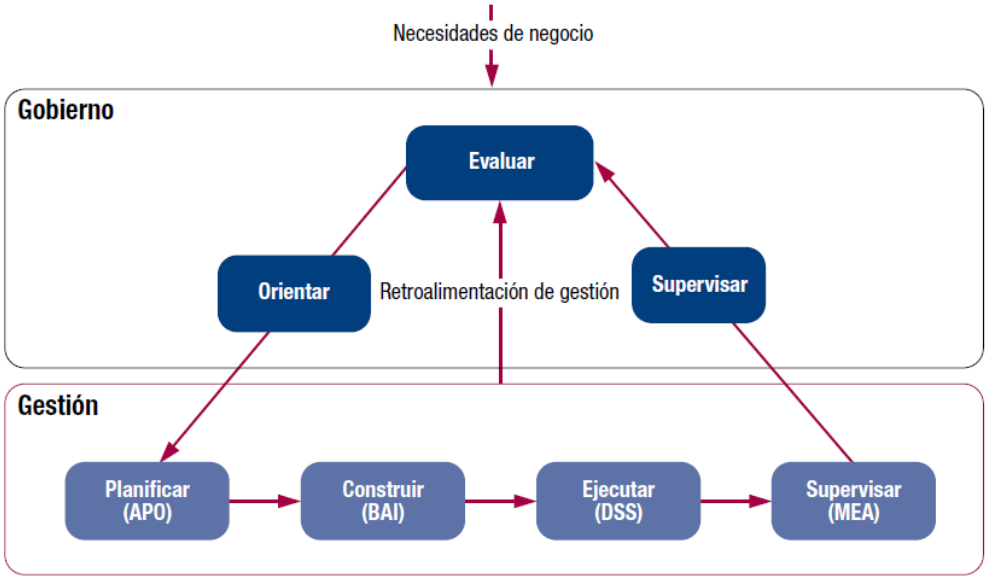
- Principios, políticas y modelos de referencia
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Gente, habilidades y competencias.

¿Cuál es la diferencia entre Gobierno y Gestión?

El gobierno asegura que los objetivos empresariales se logran evaluando las necesidades de los accionistas, las condiciones y opciones; establecer la dirección a través de la priorización y la toma de decisiones; y monitorear el desempeño, el cumplimiento y el progreso versus la dirección y objetivos acordados (*EDM*, por Evaluar, Dirigir, Monitorear).

Por su parte la gestión se ocupa de planificar, construir, ejecutar y monitorear las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales (*PBRM*: Planificar, Construir, Ejecutar y Monitorear, por su sigla en inglés).

GRÁFICO Nº 2: ÁREAS CLAVES DE GOBIERNO Y GESTIÓN COBIT 5



Fuente: http://estratega.org/todo-lo-que-usted-queria-saber-sobre-cobit-5-y-no-se-animo-a-preguntar/

¿Es COBIT 5 un modelo superior a otros modelos de control aceptados?

La mayoría de los ejecutivos conocen la importancia de los marcos generales de control en relación con la responsabilidad fiduciaria, tales como COSO, Cadbury, CoCo, Sarbanes-Oxley. Sin embargo, no necesariamente son conscientes del nivel de detalle de cada uno. Por otro lado, los ejecutivos cada vez más conocen la importancia de guías técnicas como ITIL (para la gestión de servicios de TI) e ISO 27001 (para seguridad de información).

Si bien estos estándares y modelos enfatizan el control del negocio y la seguridad y servicio de TI, COBIT es el único que se ocupa de los controles específicos de TI desde la perspectiva del negocio. De hecho, COBIT 5 se basa en ISO/IEC 15504 e ITIL. No

> se pretende que COBIT reemplace estos modelos de control, sino lo que se destacan son los elementos de gobierno y gestión y las prácticas necesarias para crear valor para la compañía. (Sperat, s.f.)

Para el autor COBIT 5 es un modelo para la gestión seguridad de la información basado en una perspectiva de gobierno y gestión; es decir una guía práctica para el mejoramiento de la seguridad de la empresa; mediante la administración adecuada de las tecnologías de información.

1.16 ¿Qué son las MPYME?

Se conoce como MPYMES al conjunto de micro, pequeñas y medianas empresas que, de acuerdo a su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos presentan características propias de este tipo de entidades económicas. Por lo general en nuestro país las micro, pequeñas y medianas empresas que se han formado realizan diferentes tipos de actividades económicas, entre las que se puede destacar las siguientes:

- Comercio al por mayor y al por menor.
- Agricultura, silvicultura y pesca.
- Industrias manufactureras.
- Construcción.
- Transporte, almacenamiento, y comunicaciones.
- Bienes inmuebles y servicios prestados a las empresas.
- Servicios comunales, sociales y personales.

Importancia de las PYMES

Las PYMES en nuestro país se encuentran en particular en la producción de bienes y servicios, siendo la base del desarrollo social del país tanto produciendo, demandando y comprando

productos o añadiendo valor agregado, por lo que se constituyen en un actor fundamental en la generación de riqueza y empleo. (SRI, s.f.)

Categorización de las PYMES en el Ecuador

- **Microempresas:** emplean hasta 10 trabajadores, y su capital fijo (descontado edificios y terrenos) puede ir hasta 20 mil dólares.
- **Talleres artesanales:** Se caracterizan por tener una labor manual, con no más de 20 operarios y un capital fijo de 27 mil dólares.
- **Pequeña Industria:** Puede tener hasta 50 obreros.
- **Mediana Industria:** Alberga de 50 a 99 obreros, y el capital fijo no debe sobrepasar de 120 mil dólares.
- **Grandes Empresas:** Son aquellas que tienen más de 100 trabajadores y 120 mil dólares en activos fijos. (Morales, 2012)

Según el autor las pequeñas y medianas empresas son el pilar fundamental para el desarrollo de la provincia y el país, así mismo, hoy en día se ha incluido el concepto de MPYME, en donde se incluyen a las micro-empresas; las mismas que tienen límites ocupacionales y financieros.

CAPÍTULO II

2.1 Análisis de la Gestión de Riesgos de TI - COSO III

Según (AUDITOOL, 2013), indica que: "Las empresas deben implementar un sistema de control interno eficiente que les permita enfrentarse a los rápidos cambios del mundo de hoy, y permita enfrentar los riesgos. El marco integrado de control interno propuesto por COSO provee un enfoque integral y herramientas para la implementación de un sistema de control interno efectivo y en pro de mejora continua. Un sistema de control interno efectivo reduce a un nivel aceptable el riesgo de no alcanzar un objetivo de la entidad".

El modelo de control interno COSO 2013 actualizado está compuesto por los cinco componentes y 17 principios los mismos que establecen las mejores prácticas para llevar a cabo con control interno de la organización; a continuación, se detallan los mismos:

2.1.1 Componente 1 - Entorno de control

2.1.1.1 Principio 1: La organización demuestra compromiso con la integridad y los valores éticos

Establece el tono de la gerencia, la Junta Directiva. La Alta Gerencia y el personal supervisor están comprometidos con los valores y principios éticos y los refuerzan en sus actuaciones.

Establece estándares de conducta. Las expectativas de la Junta Directiva y la Alta Dirección con respecto a la integridad y los valores éticos, son definidos en los estándares de conducta de la entidad y entendidos en todos los niveles de la organización y por los proveedores de servicio externos y socios de negocios.

Evalúa la adherencia a estándares de conducta. Los procesos están en su lugar para evaluar el desempeño de los individuos y equipos en relación con los estándares de conducta esperados de la entidad.

Aborda y decide sobre desviaciones en forma oportuna. Las desviaciones de los estándares de conducta esperados en la entidad son identificadas y corregidas oportuna y adecuadamente. (AUDITOOL, 2013)

2.1.1.2 Principio 2: El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.

Establece las responsabilidades de supervisión de la dirección. Aquí, la Junta Directiva identifica y acepta su responsabilidad de supervisión con respecto a establecer requerimientos y expectativas.

Aplica experiencia relevante. La Junta directiva define, mantiene y periódicamente evalúa las habilidades y experiencia necesaria entre sus miembros para que puedan hacer preguntas de sondeo de la Alta Dirección y tomar medidas proporcionales.

Conserva o delega responsabilidades de supervisión, y opera de manera independiente. Así, la Junta Directiva tiene suficientes miembros, quienes son independientes de la Administración y objetivos en evaluaciones y toma de decisiones.

Brinda supervisión sobre el Sistema de Control Interno. La Junta Directiva conserva la responsabilidad de supervisión del diseño, implementación y conducción del Control Interno de la Administración:

- Entorno de Control: establece integridad y valores éticos, estructuras de supervisión, autoridad y responsabilidad, expectativas de competencia, y rendición de cuentas a la Junta.
- Evaluación de Riesgos: monitorea las evaluaciones de riesgos de la administración para el cumplimiento de los objetivos, incluyendo el impacto potencial de los

cambios significativos, fraude, y la evasión del control interno por parte de la administración.

- Actividades de Control: provee supervisión a la Alta Dirección en el desarrollo y cumplimiento de las actividades de control.
- Información y Comunicación: analiza y discute la información relacionada con el cumplimiento de los objetivos de la entidad.
- Actividades de Supervisión: evalúa y supervisa la naturaleza y alcance de las actividades de monitoreo y la evaluación y mejoramiento de la administración de las deficiencias. (AUDITOOL, 2013)

2.1.1.3 Principio 3: Establece estructura, autoridad y responsabilidad

Considera todas las estructuras de la entidad. La Administración y la Junta Directiva consideran las estructuras múltiples utilizadas (incluyendo unidades operativas, entidades legales, distribución geográfica, y proveedores de servicios externos) para apoyar la consecución de los objetivos.

Establece líneas de reporte. La Administración diseña y evalúa las líneas de reporte para cada estructura de la entidad para permitir la ejecución de autoridades y responsabilidades y el flujo de información para gestionar las actividades de la entidad.

Define, asigna y delimita autoridades y responsabilidades.

La Administración y la Junta Directiva delegan autoridad, definen responsabilidades, y utilizan procesos y tecnologías adecuadas para asignar responsabilidad, segregar funciones según sea necesario en varios niveles de la organización:

- Junta directiva: conservar autoridad sobre las decisiones significativas y revisar las evaluaciones de la administración y las limitaciones de autoridades y responsabilidades.
- Alta Dirección: establece instrucciones, guías, y control habilitando a la administración y otro personal para entender y llevar a cabo sus responsabilidades de control interno.
- Administración: guía y facilita la ejecución de las instrucciones de la Alta Dirección dentro de la entidad y sus sub-unidades.
- Personal: entiende los estándares de conducta de la entidad, los riesgos evaluados para los objetivos, y las actividades de control relacionadas con sus respectivos niveles de la entidad, la información esperada y los flujos de comunicación, y las actividades de monitoreo relevantes para el cumplimiento de los objetivos.
- Proveedores de servicios externos: cumple con la definición de la administración del alcance de la autoridad y la responsabilidad para todos los que no sean empleados comprometidos. (AUDITOOL, 2013)

2.1.1.4 Principio 4: Demuestra compromiso para la competencia

Establece políticas y prácticas.

Las políticas y prácticas reflejan las expectativas de competencia necesarias para apoyar el cumplimiento de los objetivos.

Evalúa la competencia y direcciona las deficiencias. La Junta Directiva y la Administración evalúan la competencia a través de la organización y en los proveedores de servicios externos de acuerdo con las políticas y prácticas establecidas, y actúa cuando es necesario direccionando las deficiencias.

Atrae, desarrolla y retiene profesionales. La organización provee la orientación y la capacitación necesaria para atraer, desarrollar y retener personal suficiente y competente y proveedores de servicios externos para apoyar el cumplimiento de los objetivos.

Planea y se prepara para sucesiones. La Alta Dirección y la Junta Directiva desarrollan planes de contingencia para la asignación de la responsabilidad importante para el control interno. (AUDITOOL, 2013)

2.1.1.5 Principio 5: Hace cumplir con la responsabilidad

Hace cumplir la responsabilidad a través de estructuras, autoridades y responsabilidades.

La Administración y la Junta Directiva establecen los mecanismos para comunicar y mantener profesionales responsables para el desempeño de las responsabilidades de control interno a través de la organización, e implementan acciones correctivas cuando es necesario.

Establece medidas de desempeño, incentivos y premios. La Administración y la Junta Directiva establecen medidas de desempeño, incentivos, y otros premios apropiados para las responsabilidades en todos los niveles de la entidad, reflejando dimensiones de desempeño apropiadas y estándares de conducta esperados, y considerando el cumplimiento de objetivos a corto y largo plazo.

Evalúa medidas de desempeño, incentivos y premios para la relevancia en curso. La Administración y la Junta Directiva alinean incentivos y premios con el cumplimiento de las responsabilidades de control interno para la consecución de los objetivos.

Considera presiones excesivas. La administración y la Junta Directiva evalúan y ajustan las presiones asociadas con el cumplimiento de los objetivos, así como asignan responsabilidades, desarrollan medidas de desempeño y evalúan el desempeño.

Evalúa desempeño y premios o disciplina los individuos. La Administración y la Junta Directiva evalúan el desempeño de las responsabilidades de control interno, incluyendo la adherencia a los estándares de conducta y los niveles de competencia esperados, y proporciona premios o ejerce acciones disciplinarias cuando es apropiado. (AUDITOOL, 2013)

2.1.2 Evaluación de riesgos

2.1.2.1 Principio 6: Especifica objetivos relevantes

Objetivos Operativos:

- Refleja las elecciones de la administración.
- Considera la tolerancia al riesgo.
- Incluye las metas de desempeño operativo y financiero.
- Constituye una base para administrar los recursos.

Objetivos de Reporte Financiero Externo:

- Cumple con los estándares contables aplicables.
- Considera la materialidad.
- Refleja las actividades de la entidad.

Objetivos de Reporte no Financiero Externo:

- Cumple con los estándares y marcos externos establecidos.

- Considera los niveles de precisión requeridos.
- Refleja las actividades de la entidad.

Objetivos de Reporte interno:

- Refleja las elecciones de la administración.
- Considera el nivel requerido de precisión.
- Refleja las actividades de la entidad.

Objetivos de Cumplimiento:

- Refleja las leyes y regulaciones externas.
- Considera la tolerancia al riesgo. (AUDITOOL, 2013)

2.1.2.2 Principio 7: Identifica y analiza los riesgos

Incluye la entidad, sucursales, divisiones, unidad operativa y niveles funcionales.

La organización identifica y evalúa los riesgos a nivel de la entidad, sucursales, divisiones, unidad operativa y niveles funcionales relevantes para la consecución de los objetivos.

Evalúa la consideración de factores externos e internos en la identificación de los riesgos que puedan afectar a los objetivos.

Envuelve niveles apropiados de administración.

La dirección evalúa si existen mecanismos adecuados para la identificación y análisis de riesgos.

Analiza la relevancia potencial de los riesgos identificados y entiende la tolerancia al riesgo de la organización.

Determina la respuesta a los riesgos.

La evaluación de riesgos incluye la consideración de cómo el riesgo debería ser gestionado y si aceptar, evitar, reducir o compartir el riesgo. (AUDITOOL, 2013)

2.1.2.3 Principio 8: Evalúa el riesgo de fraude

Considera varios tipos de fraude: La evaluación del fraude considera el Reporting fraudulento, posible pérdida de activos y corrupción.

La evaluación del riesgo de fraude evalúa incentivos y presiones.

La evaluación del riesgo de fraude tiene en consideración el riesgo de fraude por adquisiciones no autorizadas, uso o enajenación de activos, alteración de los registros de información, u otros actos inapropiados.

La evaluación del riesgo de fraude considera cómo la dirección u otros empleados participan en, o justifican, acciones inapropiadas. (AUDITOOL, 2013)

2.1.2.4 Principio 9: Identifica y analiza cambios importantes

Evalúa cambios en el ambiente externo.

El proceso de identificación de riesgos considera cambios en los ambientes regulatorio, económico, y físico en los que la entidad opera.

Evalúa cambios en el modelo de negocios. La organización considera impactos potenciales de las nuevas líneas del negocio, composiciones alteradas dramáticamente de las líneas existentes de negocios, operaciones de negocios adquiridas o de liquidación en el sistema de control interno, rápido crecimiento, el cambio de dependencia en geografías extranjeras y nuevas tecnologías.

Evalúa cambios en liderazgo.

La organización considera cambios en administración y respectivas actitudes y filosofías en el sistema de control interno. (AUDITOOL, 2013)

2.1.3 Actividades de control

2.1.3.1 Principio 10: Selecciona y desarrolla actividades de control

Se integra con la evaluación de riesgos. Las actividades de control ayudan a asegurar que las respuestas a los riesgos que direccionan y mitigan los riesgos son llevadas a cabo.

Considera factores específicos de la entidad. La administración considera cómo el ambiente, complejidad, naturaleza y alcance de sus operaciones, así como las características específicas de la organización, afectan la selección y desarrollo de las actividades de control.

Determina la importancia de los procesos del negocio. La administración determina la importancia de los procesos del negocio en las actividades de control.

Evalúa una mezcla de tipos de actividades de control. Las actividades de control incluyen un rango y una variedad de controles que pueden incluir un equilibrio de enfoques para mitigar los riesgos teniendo en cuenta controles manuales y automatizados, y controles preventivos y de detección.

Considera en qué nivel las actividades son aplicadas. La administración considera las actividades de control en varios niveles de la entidad Direcciona la segregación de funciones.

La administración segrega funciones incompatibles, y donde dicha segregación no es práctica, la administración selecciona y desarrolla actividades de control alternativas. (AUDITOOL, 2013)

2.1.3.2 Principio 11: Selecciona y desarrolla controles generales sobre tecnología

Determina la relación entre el uso de la tecnología en los procesos del negocio y los controles generales de tecnología: La dirección entiende y determina la dependencia y la vinculación entre los procesos de negocios, las actividades de control automatizadas y los Controles Generales de tecnología.

Establece actividades de control para la infraestructura tecnológica relevante: la Dirección selecciona y desarrolla actividades de control diseñadas e implementadas para ayudar a asegurar la completitud, precisión y disponibilidad de la tecnología.

Establece las actividades de control para la administración de procesos relevantes de seguridad: la dirección selecciona y desarrolla actividades de control diseñadas e implementadas para restringir los derechos de acceso, con el fin de proteger los activos de la organización de amenazas externas.

Establece actividades de control relevantes para los procesos de adquisición, desarrollo y mantenimiento de la tecnología: la dirección selecciona y desarrolla actividades de control sobre la adquisición, desarrollo y mantenimiento de la tecnología y su infraestructura. (AUDITOOL, 2013)

2.1.3.3 Principio 12: Se implementa a través de políticas y procedimientos

Establece políticas y procedimientos para apoyar el despliegue de las directivas de la administración: la administración establece actividades de control que están construidas dentro de los procesos del negocio y las actividades del día a día de los empleados a través de políticas estableciendo lo que se espera y los procedimientos relevantes especificando acciones.

Establece responsabilidad y rendición de cuentas para ejecutar las políticas y procedimientos: la administración establece la responsabilidad y rendición de cuentas para las actividades de control con la administración (u otro personal asignado) de la unidad de negocios o función en el cual los riesgos relevantes residen.

Funciona oportunamente: el personal responsable desarrolla las actividades de control oportunamente, como es definido en las políticas y procedimientos.

Toma acciones correctivas: el personal responsable investiga y actúa sobre temas identificados como resultado de la ejecución de actividades de control.

Trabaja con personal competente: personal competente con la suficiente autoridad desarrolla actividades de control con diligencia y continúa atención.

Reevalúa políticas y procedimientos: la administración revisa periódicamente las actividades de control para determinar su continua relevancia, y las actualiza cuando es necesario. (AUDITOOL, 2013)

2.1.3.4 Principio 13: Usa información Relevante

Identifica los requerimientos de información: un proceso está en ejecución para identificar la información requerida y esperada para apoyar el funcionamiento de los otros componentes del control interno y el cumplimiento de los objetivos de la entidad.

Captura fuentes internas y externas de información: los sistemas de información capturan fuentes internas y externas de información.

Procesa datos relevantes dentro de la información: los sistemas de información procesan datos relevantes y los transforman en información.

Mantiene la calidad a través de procesamiento: los sistemas de información producen información que es oportuna, actual, precisa, completa, accesible, protegida, verificable y retenida. La información es revisada para evaluar su relevancia en el soporte de los componentes de control interno.

Considera costos y beneficios: la naturaleza, cantidad y precisión de la información comunicada están acorde con, y apoyan, el cumplimiento de los objetivos. (AUDITOOL, 2013)

2.1.4 Sistemas de información

Principio 14: Comunica internamente

Comunica la información de control interno: un proceso está en ejecución para comunicar la información requerida para permitir que todo el personal entienda y lleve a cabo sus responsabilidades de control interno.

Se comunica con la Junta directiva: existe comunicación entre la administración y la Junta Directiva; por lo tanto, ambas partes tienen la información necesaria para cumplir con sus roles con respecto a los objetivos de la entidad.

Proporciona líneas de comunicación separadas: separa canales de comunicación, como líneas directas de denuncia de irregularidades, las cuales sirven como mecanismos a prueba de fallos para permitir la comunicación anónima o confidencial cuando los canales normales son inoperantes o ineficientes.

Selecciona métodos de comunicación relevantes: los métodos de comunicación consideran tiempo, público y la naturaleza de la información. (AUDITOOL, 2013)

Principio 15: Comunica externamente

Se comunica con grupos de interés externos: los procesos están en funcionamiento para comunicar información relevante y oportuna a grupos de interés externos, incluyendo accionistas, socios, propietarios, reguladores, clientes, analistas financieros y demás partes externas.

Permite comunicaciones de entrada: canales de comunicación abiertos permiten los aportes de clientes, consumidores, proveedores, auditores externos, reguladores, analistas financieros, entre otros, y proporcionan a la administración y Junta Directiva información relevante.

Se comunica con la Junta Directiva: la información relevante resultante de evaluaciones conducidas por partes externas es comunicada a la Junta Directiva.

Proporciona líneas de comunicación separadas: separa canales de comunicación, como líneas directas de denuncia de irregularidades, las cuales sirven como mecanismos a prueba de fallos para permitir la comunicación anónima o confidencial cuando los canales normales son inoperantes o ineficientes.

Selecciona métodos de comunicación relevantes: los métodos de comunicación consideran el tiempo, público, y la naturaleza de la comunicación y los requerimientos y expectativas legales, regulatorias y fiduciarias. (AUDITOOL, 2013)

2.1.5 Supervisión del sistema de control - Monitoreo

2.1.5.1 Principio 16: Conduce evaluaciones continuas y/o independientes

Considera una combinación de evaluaciones continuas e independientes: la administración incluye un balance de evaluaciones continúas e independientes **Considera tasa de cambio:** la administración considera la tasa de cambio en el negocio y los procesos del negocio cuando selecciona y desarrolla evaluaciones continuas e independientes.

Establece un punto de referencia para el entendimiento: el diseño y estado actual del sistema de control interno son usados para establecer un punto de referencia para las evaluaciones continuas e independientes.

Uso de personal capacitado: los evaluadores que desarrollan evaluaciones continuas e independientes tienen suficiente conocimiento para entender lo que está siendo evaluado.

Se integra con los procesos del negocio: las evaluaciones continuas son construidas dentro de los procesos del negocio y se ajustan a las condiciones cambiantes.

Ajusta el alcance y la frecuencia: la administración cambia el alcance y la frecuencia de las evaluaciones independientes dependiendo el riesgo.

Evalúa objetivamente: las evaluaciones independientes son desarrolladas periódicamente para proporcionar una retroalimentación objetiva. (AUDITOOL, 2013)

2.1.5.2 Principio 17: Evalúa y comunica deficiencias

Evalúa resultados: la Administración o la Junta Directiva, según corresponda, evalúa los resultados de las evaluaciones continuas e independientes.

Comunica deficiencias: las deficiencias son comunicadas a las partes responsables para tomar las acciones correctivas y a la Alta Dirección y la Junta Directiva, según corresponda.

Supervisa acciones correctivas: la administración monitorea si las deficiencias son corregidas oportunamente. (AUDITOOL, 2013)

2.2 Proceso de Administración de Riesgos de TI:

Según (Maxitana & Naranjo, 2005) El proceso de administración de riesgos se realiza con las siguientes etapas que se describen a continuación:

- Establecimiento de la Metodología de TI
- Identificación de Riesgos de TI
- Análisis de Riesgo de TI
- Evaluación y Priorización de Riesgos de TI
- Tratamiento de Riesgos de TI (Controles Definitivos)
- Monitoreo y Revisión

2.2.1 Establecer Metodología

Luego de una evaluación de las diferentes metodologías que existen para analizar y administrar el Riesgo de Tecnología de Información, se ha considerado el estudio basado en el control interno, que incluye la gestión de riesgos, lo cual está se estable en la norma COSO III.

2.2.2 Identificar Riesgos de TI

En este punto se define los objetivos y el alcance del trabajo a realizar, en base a estos se desarrolla criterios de evaluación de riesgos de TI.

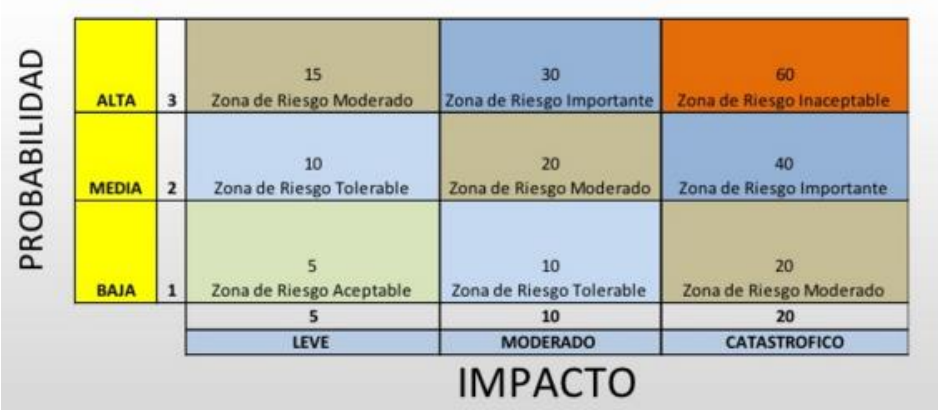
Para la identificación de los riesgos, los encargados de gestión de riesgo de TI o los auditores, deben analizar los problemas que afectan a los departamentos Informáticos y de soporte de TI en las empresas. Con esta información se establece una Matriz de Ponderación para determinar los riesgos más relevantes.

2.2.3 Análisis del Riesgo de TI

Valorar el Riesgo Inherente:

Para la valoración de los riesgos que se analizan, es importante definir una escala de valoración Cualitativa, ya que con esto se podrá evaluar las características de los mismos, permitiendo priorizarlos. Algunas metodologías sugieren trabajar en escalas de 0 al 10, y otras, de manera más consolidada, sugieren valorarlas en tres niveles: Alto, Medio y Bajo.

GRÁFICO Nº 3: VALORAR RIESGO



Fuente: http://es.slideshare.net/xhagix/riesgos-2012

Determinar Controles Existentes:

En este punto se debe verificar y establecer si el Departamento de TI, tiene ciertos controles que permitan gestionar los riesgos o carece de ellos. Estos deben prevenir, detectar o corregir la materialización de los riesgos.

Identificar Nivel de Exposición:

Para identificar este nivel se debe tener en cuenta que el Nivel de Exposición es igual a decir Riesgo Inherente menos Controles. Teniendo en cuenta esta definición, se puede indicar el nivel de riesgo que tiene una determinada empresa.

2.2.4 Evaluación y Priorización de los Riesgos: Método Matricial para el Análisis de Riesgos

Este método utiliza una matriz que muestra gráficamente tanto las amenazas a que están expuestos los sistemas computarizados y la información del departamento, como los objetos que comprenden el departamento de Sistemas.

Se describe a continuación los pasos para el desarrollo del método:

- Crear la matriz de amenazas (causas de riesgo) y de objetos del sistema a analizar.
- Categorizar los riesgos.

2.2.4.1 Crear la matriz de amenazas y de objetos

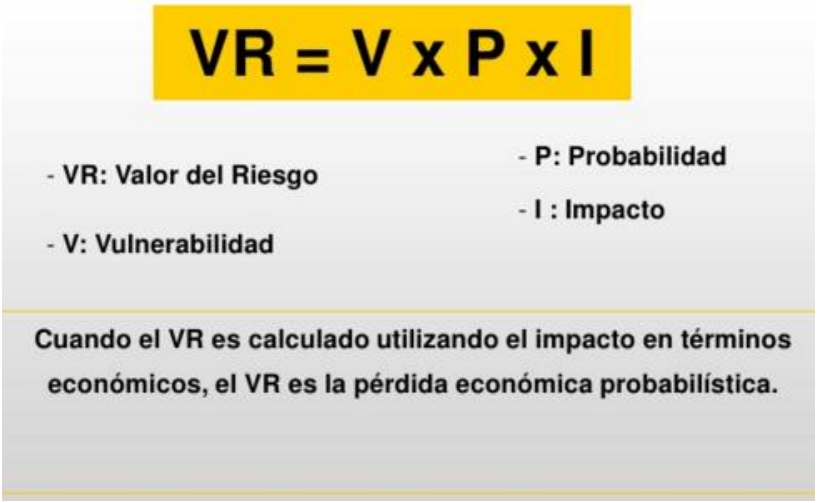
Luego de ponderar los riesgos existentes dentro del Departamento, trabajo realizado por el grupo de experto, se determinaron los que compondrán la Matriz de Control de Riesgos (Amenazas y Objetos).

2.2.4.2 Categorización de Riesgos:

Se categorizan las amenazas por niveles de riesgo, de mayor a menor en orden de importancia, como haya sido determinado por el sistema COSO III.

Luego se comienza a elaborar la matriz de riesgos, para lo cual se debe analizar secuencialmente cada uno de los procesos. A continuación, se procede a categorizar la sensibilidad de los objetos, para lo cual se utiliza como criterio la percepción de los objetos que puedan causar mayor pérdida económica si se daña o causa demoras en el procesamiento.

GRÁFICO Nº 4: FÓRMULA PARA CATEGORIZACIÓN DE RIESGO



Fuente: http://es.slideshare.net/xhagix/riesgos-2012

GRÁFICO Nº 5: MATRIZ DE RIESGO

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Base de Datos de Cobranzas	Fraude	Muy Alta	Seria	Extremo
Base de Datos de Finanzas	Incumplimiento legales	Alta	Significativa	Alto
Base de Datos de Marketing	Fuga de información	Medio	Menor	Bajo

Activo	Amenaza	Proceso	Vulnerabilidad	Probabilidad	Impacto	Valor del Riesgo
Base de Datos Finanzas	Fraude	Negociaciones	0,2	0,01	100000	200
Base de Datos Marketing	Robo	Fidelizacion de Clientes	0,1	0,01	50000	50

Fuente: http://es.slideshare.net/xhagix/riesgos-2012

2.2.5 Diseñar los controles definitivos

Finalmente, con el resultado del trabajo realizado, y apoyándose en la metodología COSO III y en el modelo matricial Riesgo / Sensibilidad, se diseñan y documentan definitivamente los controles a nivel: preventivo, detectivo y correctivo; de acuerdo al área informática del Departamento de Sistemas.

2.2.6 Presentar los Resultados

La empresa debe conocer el resultado del análisis de riesgo de manera oportuna, el cual será presentado en un informe detallado. De esta manera la Gerencia General podrá tomar las acciones necesarias para su implantación.

Como ya se puntualizó al inicio del presente capítulo el contenido del informe para el control interno, según COSO III, está compuesto por los cinco componentes, y 17 principios que la administración de toda organización debería implementar.

2.3 COSO III relación con las normas ISO

Según (Sánchez, 2015), indica que COSO tiene como misión: "Proporcionar liderazgo a través de la elaboración de modelos y guías en materias de administración de riesgos (ERM), control interno y disuasión del fraude; diseñados para mejorar el desempeño y la gobernanza institucional, así como para reducir el fraude en las organizaciones."

Entonces COSO es un marco integrado de control interno organizacional, que reúne las mejores prácticas para administrar de forma eficaz la empresa, asegurando el alcance de los objetivos propuestos; esta norma nace con el propósito de estandarización de normas y políticas del control interno de las instituciones.

GRÁFICO Nº 6: RELACIÓN DE COSO III CON LAS NORMAS ISO – PARTE 1 - 2

Entorno de Control	1. Compromiso de la organización. 2. El consejo de administración es independencia y supervisa el desempeño del sistema de control interno. 3. La dirección establece, con la supervisión del consejo, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados. 4. La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes. 5. La organización define las responsabilidades de las personas a nivel de control interno.	Involucrar a la entidad	Involucrar a la entidad	Definición del contexto organizacional interno y externo	Marco de trabajo o framework
Evaluación de Riesgos	6. La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados. 7. La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determinar cómo se deben gestionar. 8. La organización considera la probabilidad de fraude al evaluar los riesgos. 9. La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.	Elegir el método de evaluación de riesgo Identificar, analizar y evaluar los riesgos Determinar la política y el alcance		Valoración de riesgos tecnológicos	Evaluación de riesgo
Actividades de Control	10. La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables.	Definir acciones y objetivos para gestionar los riesgos	Política de la Información Normas y políticas de un SGSI Adquisición, desarrollo y mantenimiento de sistemas de información. Seguridad Física	Tratamiento de riesgos tecnológicos	

GRÁFICO Nº 7: RELACIÓN DE COSO III CON LAS NORMAS ISO – PARTE 2 - 2

	11. La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología.		Control del Acceso		
	12. La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos.		Seguridad de los Recursos Humanos		
Información y Comunicación	13. La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.	Educar a los empleados y asignar recursos	Organización de la seguridad	Establecimiento de un plan de comunicación interno y externo	
	14. La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.		Gestión de Comunicaciones y Operaciones		
	15. La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.				
Actividades de Supervisión	16. La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.	Auditoría interna, revisión gerencial y mejoras	Gestión de la Continuidad del Negocio	Monitoreo y mejora continua del proceso de gestión	Monitorización y revisión.
	17. La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda.		Gestión de los incidentes de la seguridad de la información		
COSO III		ISO 27001	ISO 27002	ISO 27005	ISO 31000

Fuente: Elaborado por el autor**.**

Según (taringa.net, 2011) “C.O.S.O. es un comité (Comité de Organizaciones Patrocinadoras de la Comisión Treadway) que redactó un informe que orienta a las organizaciones y gobiernos sobre control interno, gestión del riesgo, fraudes, ética empresarial, entre otras. Dicho documento es conocido como “Informe C.O.S.O.” y ha establecido un modelo común de control interno con el cual las organizaciones pueden evaluar sus sistemas de control”.

Para el desarrollo de la matriz relacional o integración de COSO III con las normas ISO establecidas en los objetivos de la investigación, se realizó a partir de los diferentes conceptos que se relacionan con las diferentes normas ISO; esto porque COSO también es creado en base a estas normas, ya que el informe de COSO III reúne las mejores prácticas que engloban a todas las áreas de la empresa y la mayoría de las normas ISO es para gestionar una determinada área de la empresa; de esta manera COSO es creado por expertos en el tema con el objetivo de estandarizar las políticas de control interno, gestión de riesgo, fraudes, entre otros, guiando de manera correcta a las empresas a conseguir sus metas.

2.4 Conclusión

La gestión de riesgos es muy importante en todo ámbito, especialmente en organizaciones que hoy día trabajan en base a los nuevos avances tecnológicos que ayudan a realizar sus procesos de manera eficaz; gracias a las diferentes metodologías que reúnen las mejores prácticas para detectar y tratar los riesgos, se puede determinar el comportamiento de los riesgos en el futuro, de esta manera permitiendo mitigar la posibilidad de pérdidas económicas en dentro de la empresa.

En la actualidad toda organización debe implantar un sistema de control interno que permita adaptarse a los cambios y competitividad existente en la actualidad, estos controles tienen la finalidad de controlar y eliminar los riesgos. Una de las normas para utilizadas para realizar este proceso es el Marco integrado de control interno propuesto

por COSO, el cual provee un enfoque integral y herramientas para la implementación de un sistema de control interno efectivo, procurando el alcance de los objetivos empresariales de manera óptima, procurando la mejora continua de la prestación de servicios o procesos productivos.

Un sistema de control interno bien definido reduce los riesgos y permite que la organización puede alcanzar sus objetivos de manera oportuna. El principal objetivo de la administración de los riesgos de TI, es garantizar la estabilidad de la organización, relacionado con los objetivos empresariales.

La norma COSO se puede utilizar para la gestión de riesgos de tecnologías de la información, ya que permitirá ver de manera global los riesgos internos de la empresa, los cuales se puede relacionar con el área TI. Permitiendo que los recursos informáticos sean administrados de manera correcta satisfaciendo las necesidades de los usuarios, y minimizando a lo máximo los riesgos internos relacionados a una de las áreas primordiales de una organización que es la de sistemas.

A lo largo de la investigación se ha podido observar que COSO es una guía que contiene las mejores prácticas para erradicar los riesgos, fraudes, así como orientar a las organizaciones y gobiernos a llevar un control interno eficaz de los procesos que se realizar dentro de la institución. Esta norma ha ido evolucionando y mejorando, la versión actual tiene el nombre de COSO III; el mismo que tiene 17 principios para la creación del Informe COSO, el cual permite establecer un modelo común de control interno con el cual las organizaciones pueden evaluar sus sistemas de control; es decir esta norma engloba o abarca todas las áreas de la empresa, en cambio las normas ISO son destinadas a un área específica; por ejemplo la norma ISO 27001 describe las mejores prácticas para gestionar la seguridad de la información en una empresa, de la misma forma la norma ISO 31000 es una norma internacional para la Gestión de Riesgos, el cual proporciona principios y una guía que ayuda a las organizaciones a realizar un análisis, evaluación y gestión de riesgos con el fin de mitigar los mismos.

Entonces se puede decir COSO III, al igual que COBIT 5, parte de las normas ISO y la utilización en conjunto tanta de las normas ISO, así como el informe de COSO III, puede maximizar y fortalecer la administración y gestión de riesgos con el objetivo de guiar a la empresa hacia el éxito.

CAPITULO III

3.1 Análisis de la Gestión de Riesgos de TI – COBIT 5

3.1.1 COBIT 5 para riesgos.

En términos del Riesgo Tecnológico, existe un consenso generalizado en definirlo como: la posibilidad de pérdidas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la organización, al comprometer o degradar las dimensiones críticas de la información (Ej. confidencialidad, integridad, disponibilidad). (ISACA, 2012)

En ese sentido, COBIT 5 para Riesgos define el Riesgo de TI como "un riesgo para el negocio, específicamente el riesgo para el negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI dentro de una empresa". (ISACA, 2012)

Las organizaciones deben integrar la gestión del riesgo tecnológico en una forma mucho más efectiva y concreta dentro de la gestión del riesgo empresarial (ERM), si quieren reducir sus futuras pérdidas y mejorar la performance del negocio. (ISACA, 2012)

Una inadecuada gestión de los riesgos de TI puede reducir el valor del negocio, creando pérdidas financieras, dañando la reputación corporativa y desperdiciando nuevas oportunidades. Con ese objetivo, COBIT 5 for Risk de ISACA, fue desarrollado por un comité global de profesionales en riesgos, brindando una guía detallada para gobernar y gerenciar los Riesgos de TI. (ISACA, 2012)

Según lo expresado por Steven Babb, jefe de la Task Force de COBIT 5 for Risk, ya no alcanza con identificar un riesgo y agregarlo al registro de riesgos, es fundamental poder vincularlo directamente con el resultado de los objetivos estratégicos para el Negocio.

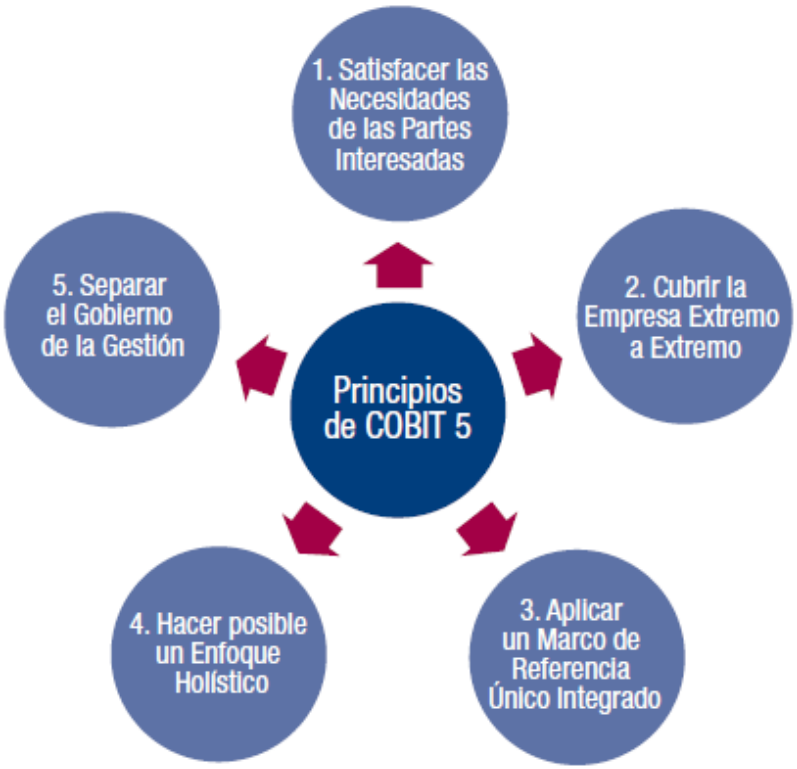
COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el

equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (ISACA, 2012)

3.1.2 Principios de COBIT 5

COBIT 5 se basa en cinco principios claves (mostrados en el gráfico Nº 6) para el gobierno y la gestión de las TI empresariales:

GRÁFICO Nº 8: PRINCIPIOS DE COBIT 5



Fuente: (ISACA, 2012)

3.1.2.1 Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. (ISACA, 2012)

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos. (ISACA, 2012)

El propósito del gobierno y administración del riesgo es ayudar a asegurar que la empresa logre sus objetivos, y la optimización de riesgos es uno de los tres componentes de la creación de valor. Las empresas existen para crear valor para sus interesados. (Ritegno, 2012)

GRÁFICO Nº 9: ADAPTABILIDAD DE COBIT 5 A LAS NECESIDADES DE LA EMPRESA MEDIANTE LA CASCADA DE METAS

Fuente: (Ritegno, 2012)

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de 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.

Las empresas existen para crear valor para sus accionistas, y 'crear valor' significa cosas diferentes — y a veces contradictorias — para cada uno de ellos.

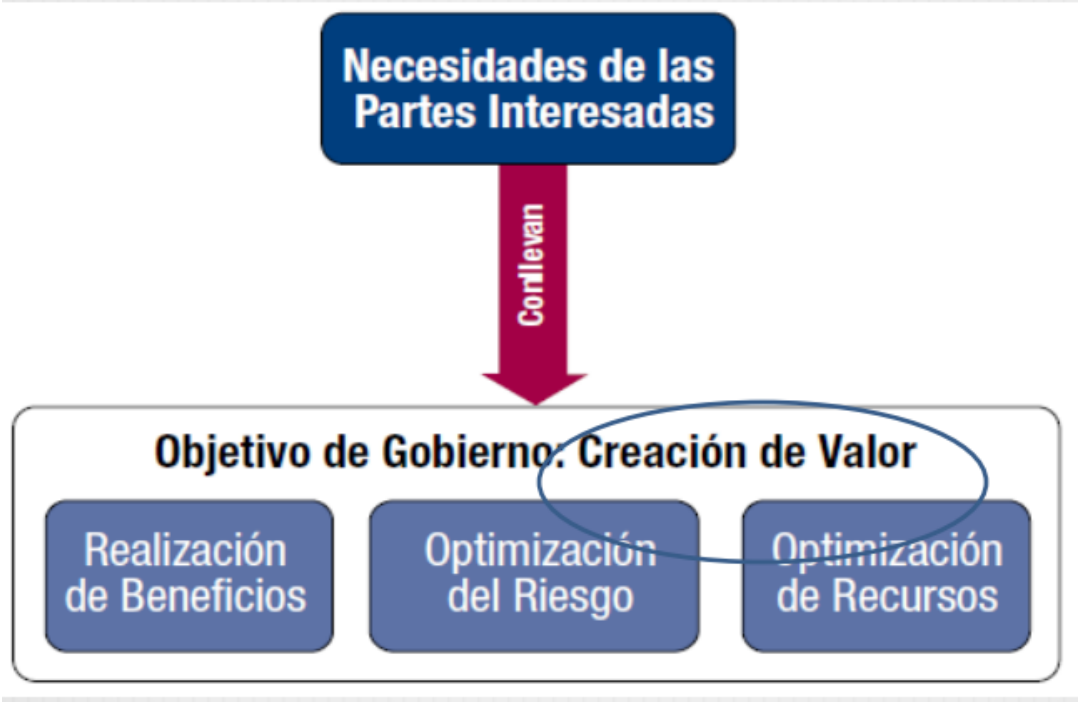
- Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas.
- En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos.
- Para cada decisión, las siguientes preguntas pueden y deben hacerse:
  - ¿Para quién son los beneficios?
  - ¿Quién asume el riesgo?
  - ¿Qué recursos se requieren?

Gestión de Riesgo la creación del valor:

Las empresas deben crear valor, como objetivo de Gobierno. Realizar los beneficios, Optimizando el uso de los recursos a la vez que se optimiza el Riesgo (Niveles de tolerancia aceptados por la política de Gobierno establecida por el directorio)

- La gestión de riesgos no puede verse como un proceso aislado
- Es parte integrante de la creación del valor
- Tiene influencia directa en los otros componentes de Gobierno

GRÁFICO Nº 10: NECESIDADES DE LAS PARTES INTERESADAS



Fuente: (Ritegno, 2012)

3.1.2.2 Principio 2: Cubrir la Empresa Extremo-a-Extremo

COBIT 5 for Risk cubre todos los habilitadores de gobierno y gestión y describe todas las fases de gobierno y gestión de riesgos e integra el gobierno y la gestión de TI en el gobierno Corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa. (ISACA, 2012)

- 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 – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas. (ISACA, 2012)

Esto significa que COBIT 5:

- Integra el gobierno empresarial de TI en el gobierno corporativo.
- Cubre todas las funciones y procesos dentro de la empresa;

3.1.2.3 Principio 3: Aplicar un Marco de Referencia único integrado

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, 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. (ISACA, 2012)

Según (ISACA, 2012), COBIT 5 for Risk se alinea con los principales marcos y estándares de administración de riesgos e integra diversos productos de COBIT, como Val IT y Risk IT y se alinea con los estándares y marcos más relevantes usados por las empresas:

- Empresariales: COSO, COSO ERM, ISO/IEC 9000,
- Relacionados con TI: ISO/IEC 38500, ITIL, serie ISO/IEC 27000, TOGAF, Etc.

Esto permite que la empresa use COBIT 5 como un marco integrador de gobierno y administración de TI.

3.1.2.4 Principio 4: Hacer Posible un Enfoque Holístico

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores o habilitadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. (ISACA, 2012)

COBIT 5 for Risk identifica todos los elementos interconectados de los habilitadores requeridos para para proveer una adecuado gobierno y gestión de riesgo. Los habilitadores de COBIT 5, Factores que, individual y colectivamente influencian para que algo funcione. En el caso de COBIT, este algo, son el gobierno y la administración de TI empresarial. (ISACA, 2012)

El marco de trabajo describe los habilitadores/catalizadores de COBIT 5 en siete categorías:

1. Principios, Políticas y marcos
2. Procesos
3. Estructuras organizacionales
4. Cultura, Ética y Conducta
5. Información
6. Servicios, Infraestructura y Aplicaciones
7. Gente, Habilidades y Competencias. (ISACA, 2012)

Catalizadores corporativos para la Gestión de Riesgo

GRÁFICO Nº 11: CATALIZADORES CORPORATIVOS

Fuente: (ISACA, 2012)

La Gestión del Riesgo (2 Procesos de Soporte).

- Evaluar Orientar y Supervisar (EDM) (Gobierno) EDM03.
- Asegurar la optimización del Riesgo Alinear Planear y Organizar (APO) (Gestión) APO12.

La Función de Riesgo (13 Procesos de Soporte)

- Gestionar los riesgos Evaluar Orientar y Supervisar (EDM) (Gobierno) EDM01
- Asegurar el establecimiento y mantenimiento de un marco de Gobierno Alinear Planear y Organizar (APO) (Gestión) APO01 Gestionar la Estrategia Fuente: (ISACA, 2012)

3.1.2.5 Principio 5: Separar el Gobierno de la Gestión

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. (ISACA, 2012)

COBIT 5 distingue entre actividades de gobierno de riesgo y gestión de riesgo.

Estas dos disciplinas:

- Incluyen diferentes tipos de actividades
- Requieren diferentes estructuras organizacionales
- Sirven para diferentes propósitos (ISACA, 2012)

La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

– **Gobierno: Responsabilidad de la Junta Directiva.** El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas

acordadas. En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas. (Ritegno, 2012)

- **Gestión: Responsabilidad de la alta administración, bajo el liderazgo del CEO.** La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO). (Ritegno, 2012)

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

3.1.3 Procesos COBIT 5 para la gestión del riesgo

COBIT 5.0 – Considera al Gobierno y la Gestión de los Riesgos como parte integrante del marco de Gestión de la Tecnología de la Información.

La gestión de riesgos es un fenómeno generalizado en toda la empresa, con aspectos de relacionados en todas las actividades y procesos realizados. Entregan metas y métricas de TI con sus actividades, relaciones y matrices RACI de responsabilidad para cada proceso. Los catalizadores corporativos son recursos corporativos que tienen que ser gestionados y gobernados. Se debe considerar un conjunto interconectado de catalizadores con el fin de alcanzar las metas corporativas. (ISACA, 2012)

Entrega prácticas de gestión o de gobierno detalladas para cada uno de los 37 procesos definidos en el modelo Son un apoyo al Gobierno de la TI y la Gestión de los Riesgos.

Perspectiva sobre el riesgo

Los catalizadores corporativos son recursos corporativos que tienen que ser gestionados y gobernados. Se debe considerar un conjunto interconectado de catalizadores con el fin de alcanzar las metas corporativas. (ISACA, 2012)

Perspectivas de la Función de Riesgo: Describe lo que se necesita en una empresa para construir y sostener actividades efectivas de gobierno y gestión de riesgos. (ISACA, 2012)

Perspectiva de la Administración de Riesgo: Describe como los procesos "core" de gestión de riesgos que son identificación, análisis, respuesta y respuesta de riesgos, pueden ser apoyadas con los habilitadores de COBIT 5. (ISACA, 2012)

Escenarios de Riesgo

Son una descripción de los eventos que afectan con un impacto no determinado en el logro de los objetivos empresariales.

1. Los objetivos de negocio se deben validar contra los posibles escenarios como parte de las actividades de análisis de Riesgo de TI (gestión Top/Down). (Ritegno, 2012)

2. La lista de escenarios de riesgo se debe utilizar para definir una cantidad de escenarios relevantes adaptados a la empresa (gestión Bottom/Up). (Ritegno, 2012)

COBIT5 establece que los Escenarios de Riesgo son una pieza de información clave para la Gestión de Riesgos (definida en el proceso APO12) y además define 20 categorías de Escenarios de Riesgo. Y mide los escenarios de riesgo en función de su impacto primario o secundario a las tres categorías de riesgo explicadas al inicio. (Ritegno, 2012)

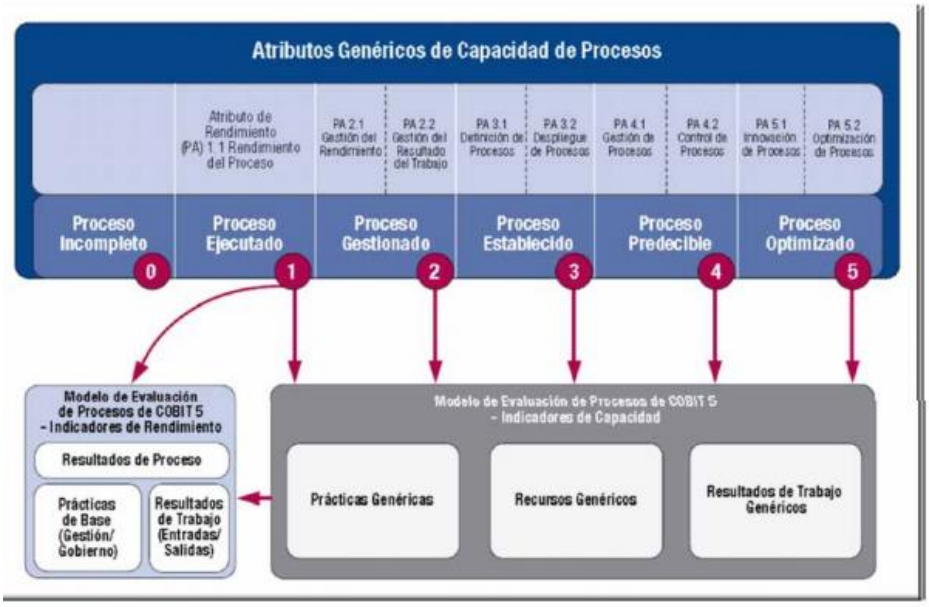
Categorías de Riesgo TI

1. Establecimiento y mantenimiento del Portfolio de Proyectos

2. La Gestión del ciclo de vida de los Proyectos

3. El Proceso decisorio de las inversiones de TI
4. Experiencia y habilidades de los recursos de TI
5. Operaciones del personal (Abusos e Intentos Maliciosos)
6. Información (Filtraciones, Perdidas, Accesos Indebidos)
7. Arquitectura de TI (Visión y Diseño)
8. Infraestructura (Hardware, Software, Selección, Implementación y Baja de Sistemas)
9. Software (Ciclo de Vida)
10. Ineficaz pertenencia del negocio de TI (Compras Departamentales, Requerimientos inadecuados)
11. Selección de Proveedores de TI
12. Cumplimiento Regulatorio
13. Geopolítica (Interferencia Gubernamental, Acciones dirigidas)
14. Robo de Infraestructura
15. Malware
16. Ataques Lógicos (Espionaje Industrial, Virus)
17. Acción Industrial (Huelgas, Paros directos o indirectos)
18. Entorno (Equipamiento no amigable con el entorno)
19. Actos de la naturaleza
20. Innovación (Tendencias)

GRÁFICO Nº 12: MODELO DE EVALUACIÓN DE PROCESOS COBIT 5



Fuente: (Ritegno, 2012)

3.2 Riesgo TI.

COBIT 5 para Riesgos presenta dos perspectivas en el uso de COBIT en un contexto de riesgo:

- **la función de riesgo**: 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. (Ritegno, 2012)

- **la gestión de riesgos:** 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. (Ritegno, 2012)

3.2.1 Factores de riesgo interno

Capacidad de Gerenciamiento de Riesgos de TI

La capacidad para administrar los riesgos de TI, es uno de los factores claves para garantizar la continuidad de la organización, para esto existen catalizadores corporativos que se asocian los mismos que:

- Tiene impacto en las decisiones de riesgo empresariales.
- Tiene impacto en la presencia o ausencia de controles y su efectividad. (Ritegno, 2012)

Capacidad de la TI

Indicador de las capacidades relacionadas a la Tecnología de la información. Un mayor nivel de madurez impacta en mayor capacidad de los procesos de TI.

- Reduce la frecuencia de los eventos
- Reduce el impacto empresarial cuando los eventos ocurren. (Ritegno, 2012)

3.2.2 Gestión de riesgos de TI

Para lograr un programa efectivo de Gestión de Riesgos de TI básicamente se debe buscar un balance enfocándose en:

- Las políticas y procesos con buenos estándares de cumplimiento de las legislaciones y regulaciones
- El soporte a los objetivos del negocio
- Integración con el Gobierno Corporativo
- Complementar estos esfuerzos con:
    - El soporte de la Tecnología de la Información.

- La educación de los recursos.

Esto se logra con un enfoque consistente, integrado y alineado con el gobierno de la empresa.

- Garantizar que las decisiones de TI se han tomado en línea con los objetivos.
- Garantizando la supervisión de los procesos de manera efectiva y transparente y el cumplimiento.
- El Riesgo de TI para administrar los múltiples escenarios de riesgo y otros muchos desafíos.
- Un buen Gobierno de TI asegurará estar alineados con los objetivos del negocio y una buena Gestión Gerencial y un monitoreo efectivo de la gestión de riesgo para mantenerse encarriladas y evitar las sorpresas. (Ritegno, 2012)

3.3 COBIT 5 relación con las normas ISO

GRÁFICO Nº 13: RELACIÓN O ALINEACIÓN DE COBIT 5 CON LAS NORMAS ISO

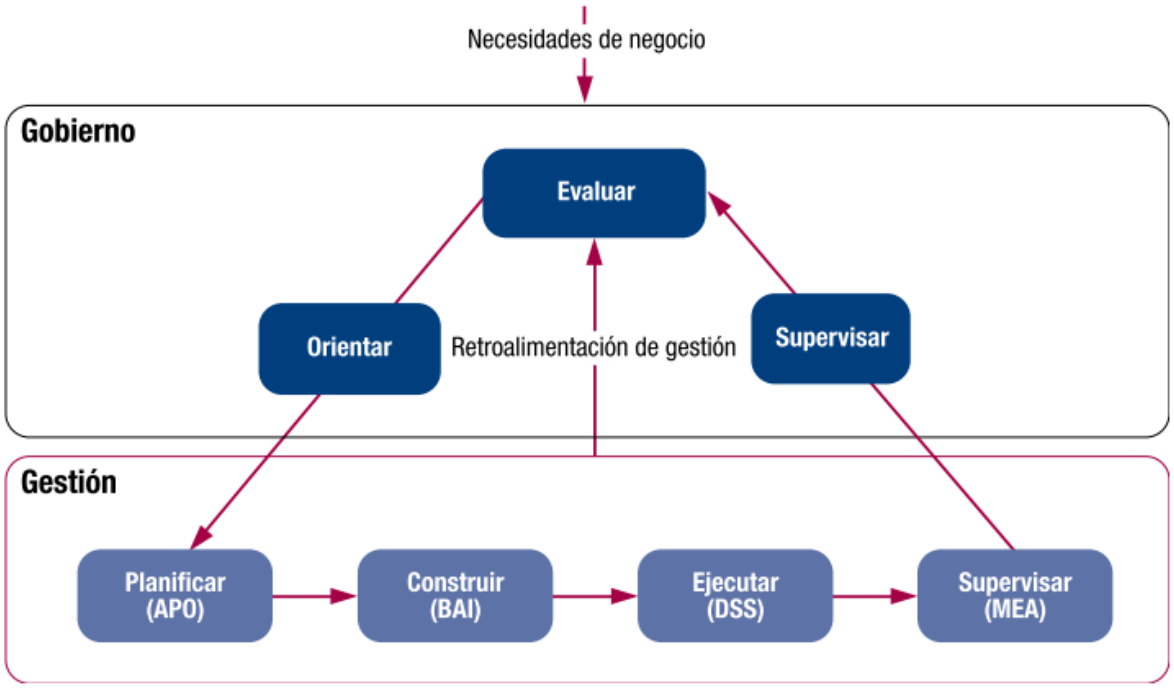
GOBIERNO	Evaluar			EDM	Evaluar los riesgos		Valoración de riesgos tecnológicos	Evaluación de riesgo
	Dirigir					Organización de la seguridad		
	Monitorizar				Auditoría interna, revisión gerencial y mejoras		Monitoreo y mejora continua del proceso de gestión	Monitorización y revisión.
GESTIÓN	Monitorear Evaluar Valorar	MEA	Alinear	APO	Involucrar a la entidad	Involucrar a la entidad	Definición del contexto organizacional interno y externo	Marco de trabajo o framework
			Planificar		Determinar la política y el alcance	Política de la Información / Normas y políticas de un SGSI	Establecimiento de un plan de comunicación interno y externo	
			Organizar		Elegir el método de evaluación de riesgo	Organización de la seguridad		
			Construir	BAI	Identificar, analizar y evaluar los riesgos	Gestión de Comunicaciones y Operaciones	Tratamiento de riesgos tecnológicos	
			Adquirir		Definir acciones y objetivos para gestionar los riesgos	Adquisición, desarrollo y mantenimiento de sistemas de información.		
			Implementar			Seguridad Física / Control del Acceso		
					Implementación de la ISO 27001	Seguridad de los Recursos Humanos		
			Entregar	DSS	Auditoría interna, revisión gerencial y mejoras			
			Servicio		Educar a los empleados y asignar recursos	Gestión de la Continuidad del Negocio	Monitoreo y mejora continua del proceso de gestión	Monitorización y revisión.
			Soporte			Gestión de los incidentes de la seguridad de la información		
COBIT 5.0					ISO 27001	ISO 27002	ISO 27005	ISO 31000

Fuente: Elaborado por autor.

En el Gráfico Nº 11 se puede visualizar la matriz de integración de COBIT5 con las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

Para la identificación de la alineación o relación de COBIT5 con las normas ISO establecidas, se partió de la premisa de COBIT 5 separa la parte de gobierno con la parte de gestión, como se muestra en la siguiente Gráfico Nº12.

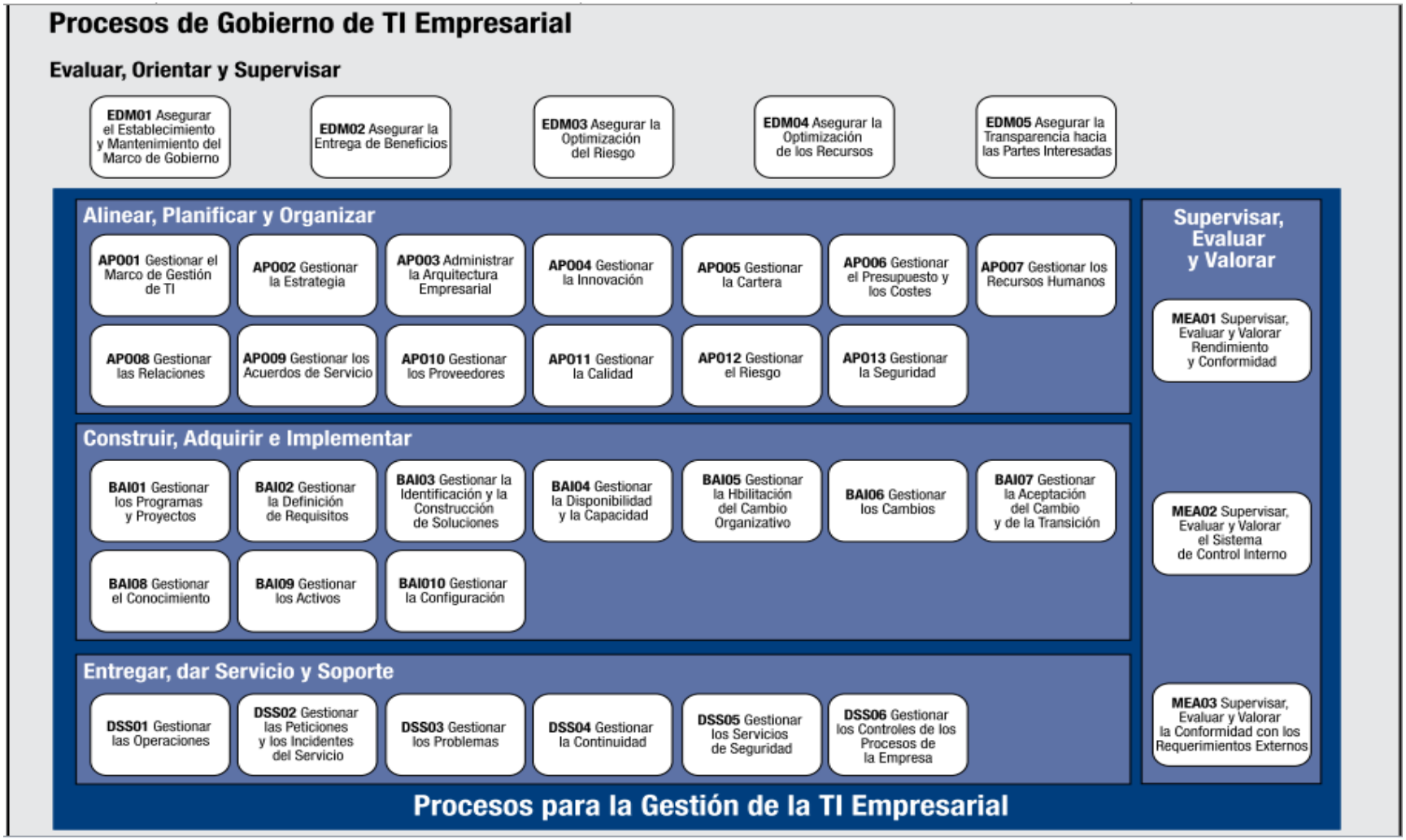
GRÁFICO Nº 14: ÁREAS CLAVES DE GOBIERNO Y GESTIÓN DE COBIT5



Fuente: (Amon, 2012, pág. 23)

Así mismo se basó en el modelo de referencia de COBIT 5 que cual se puede visualizar en el Gráfico Nº 13 en el cual el proceso o dominio **MEA** (Monitorear o Supervisar, Evaluar y Valorar) abarca los 3 dominios que son: **APO** (Alinear, Planear y Organizar), **BAI** (Construir, Adquirir e Implantar), **DSS** (Entrega, Servicio y Soporte).

GRÁFICO Nº 15: MODELO DE REFERENCIA DE PROCESOS DE COBIT 5.



Fuente: (Amon, 2012, pág. 24)

Así mismo la matriz resumida que reúne la alineación de COBIT 5 con las normas ISO se realizó a partir de los diferentes conceptos que se relacionan en las diferentes normas de estudio planteadas en la presente investigación; estas normas se han tomada como referencia y se han ido mejorando y puliendo durante la construcción de la norma COBIT 5, obteniendo así las mejores prácticas para el gobierno y gestión de la seguridad de la información.

En el Gráfico Nº 11 del presente capitulo se puede observar que existen procesos u operaciones de las normas ISO coloreadas las cuales se ha tomado como referencia en la construcción del COBIT 5 en las dos áreas tanto de gobierno como de gestión.

Finalmente, para la construcción de la matriz relacional de COBIT5 con las normas ISO de estudio se revisó la comparación realizada por (ISACA, 2012, págs. 60-61):

Comparación Con Otros Estándares

COBIT 5 se desarrolló teniendo en cuenta un número considerable de estándares y marcos de referencia.

COBIT 5: Procesos Catalizadores contiene mapeos a alto nivel entre cada proceso de COBIT 5 y las partes más relevantes de los estándares y marcos de referencia relacionados, con orientaciones adicionales.

En esta sección se incluye un breve debate sobre cada marco de trabajo o estándar, indicando a qué áreas y dominios de COBIT 5 hacen referencia.

ITIL®

Las siguientes áreas y dominios de COBIT 5 están cubiertas por ITIL:

• Un subconjunto de procesos en el domino DSS.

• Un subconjunto de procesos en el dominio BAI.

• Algunos procesos en el dominio APO.

Serie ISO/IEC 27000

Las siguientes áreas y dominios COBIT 5 están cubiertas por las ISO/IEC 27000:

• Procesos de seguridad y relativos al riesgo en los dominios EDM, APO y DSS.

• Varias actividades relacionadas con la seguridad dentro de procesos en otros dominios.

• Actividades de supervisión y evaluación del dominio MEA.

Serie ISO/IEC 31000

Las siguientes áreas y dominios COBIT 5 están cubiertas por las ISO/IEC 31000:

• Procesos relativos a la gestión del riesgo en los dominios EDM y APO.

TOGAF®

Las siguientes áreas y dominios COBIT 5 están cubiertas por TOGAF:

• Procesos relativos a los recursos en el dominio EDM (gobierno) – Los componentes TOGAF del Cuadro de la Arquitectura, Gobierno de la Arquitectura y Modelo de Madurez de la Arquitectura se mapean con la optimización de recursos.

• El proceso de arquitectura de la empresa en el dominio APO. En el núcleo de TOGAF está el ciclo del Método de Desarrollo de la Arquitectura (ADM), que se mapea con las prácticas COBIT 5 relativas al desarrollo de una visión de la arquitectura (ADM Fase A), definición de arquitecturas de referencia (ADM Fases B, C, D), selección de oportunidades y soluciones (ADM Fase E) y definición de la implementación de la arquitectura (ADM Fases F, G).

Varios componentes de TOGAF se mapean con la práctica COBIT 5 de provisión de servicios para la arquitectura de la empresa. Esto incluye:

– Gestión de los Requisitos ADM.

– Principios de Arquitectura.

– Gestión de las Partes Interesadas.

– Evaluación de la Disposición a la Transformación del Negocio.

– Gestión del Riesgo.

– Planificación basada en las Capacidades.

– Conformidad con la Arquitectura.

– Contratos de Arquitectura.

Integración de Modelos de Madurez de las Capacidades (CMMI) (desarrollo)

Las siguientes áreas y dominios COBIT 5 están cubiertas por CMMI:

• Procesos relativos a la construcción y adquisición de aplicaciones en el dominio BAI.

• Algunos procesos organizativos y relativos a la calidad del dominio APO.

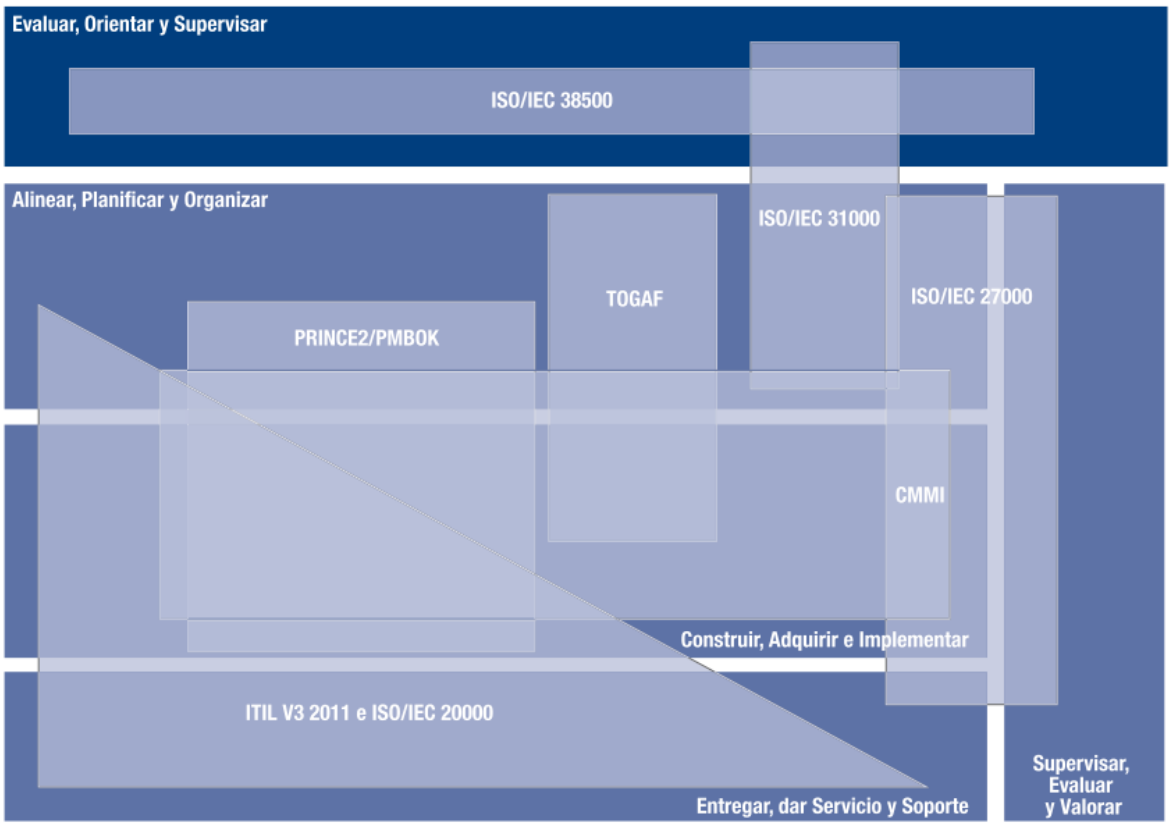
PRINCE2®

Las siguientes áreas y dominios COBIT 5 están cubiertas por PRINCE2:

• Los procesos relativos al portafolio en el dominio APO.

• Procesos de gestión de procesos y programa en el dominio BAI.

GRÁFICO Nº 16: COBERTURA DE COBIT 5 CON OTROS ESTÁNDARES Y MARCOS DE TRABAJO



Fuente: (ISACA, 2012, pág. 61)

Como se puede apreciar el Gráfico Nº 14 para la construcción de COBIT5 se basó en muchos otros estándares y marcos de referencia, reuniendo las características más relevantes, con el fin de obtener una norma robusta adaptable a cualquier tipo de organización sea pequeña, mediana o grande.

La creación de COBIT5 es realizada por varios expertos que pertenecen a la fuerza de trabajo de ISACA (Asociación de Control y Auditoria de Sistemas de Información), durante el desarrollo de esta norma han ido puliendo y mejorando las normas en base a sus experiencias y criterios; lo cual dificulta un poco saber la relación exacta de las normas ISO y COBIT5, es por ello que en la presente investigación se revisó varios

factores para determinar la matriz comparativa de alineación con las normas ISO, una de ellas fue por los conceptos que se relacionan.

Según (ISACA, 2012, pág. 2) indica que: "actualiza continuamente el COBIT®, el cuál ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio".

3.4 Conclusión

La Tecnología hoy por hoy está involucrada en todos aspectos de la vida personal e institucional y uno de los recursos que permite manejar son la información que es uno de los recursos más importantes para todas las organizaciones; gracias a los nuevos avances en el área de la informática, existen los sistemas de información que almacenas y permiten la gestión de la datos; pero no todo es 100% seguro, ya que existen muchos riesgos o vulnerabilidades a las cuales hay que atacar con el fin de procurar la estabilidad y continuidad de las empresas, asegurando que los objetivos de cumplan y las inversiones realizadas no sean en vano.

Por tales motivos se ha creado la norma COBIT 5 que reúne las mejores prácticas para la gestión de los riesgos de tecnología de la información, permitiendo alcanzar la excelencia operativa, a través de uso adecuado y oportuno de la tecnología, manteniendo el riesgo relacionado con TI en niveles aceptables.

COBIT 5 es desarrollada a partir de las diferentes normas ISO, en base a ellas los expertos han dividido en 2 partes fundamentales de gestión que es la de **gobierno y administración,** la cuales permiten una gestión integral; asegurando el alcance de los objetivos organizacionales. En definitiva, esta norma ha nacido para ayudar a las

organizaciones a crecer a partir de la TI, manteniendo una relación con los objetivos institucionales predefinidos y la gestión de los niveles de riesgo a través de la buena utilización de los recursos de TI.

El Gobierno es el encargado de velar por el logro de los objetivos de la institución, por medio de la evaluación de las necesidades de los usuarios involucrados referentes a la TI; así como monitorear el desempeño, cumplimiento y progreso en las actividades predispuestas, que permiten el alcance de los objetivos de la organización.

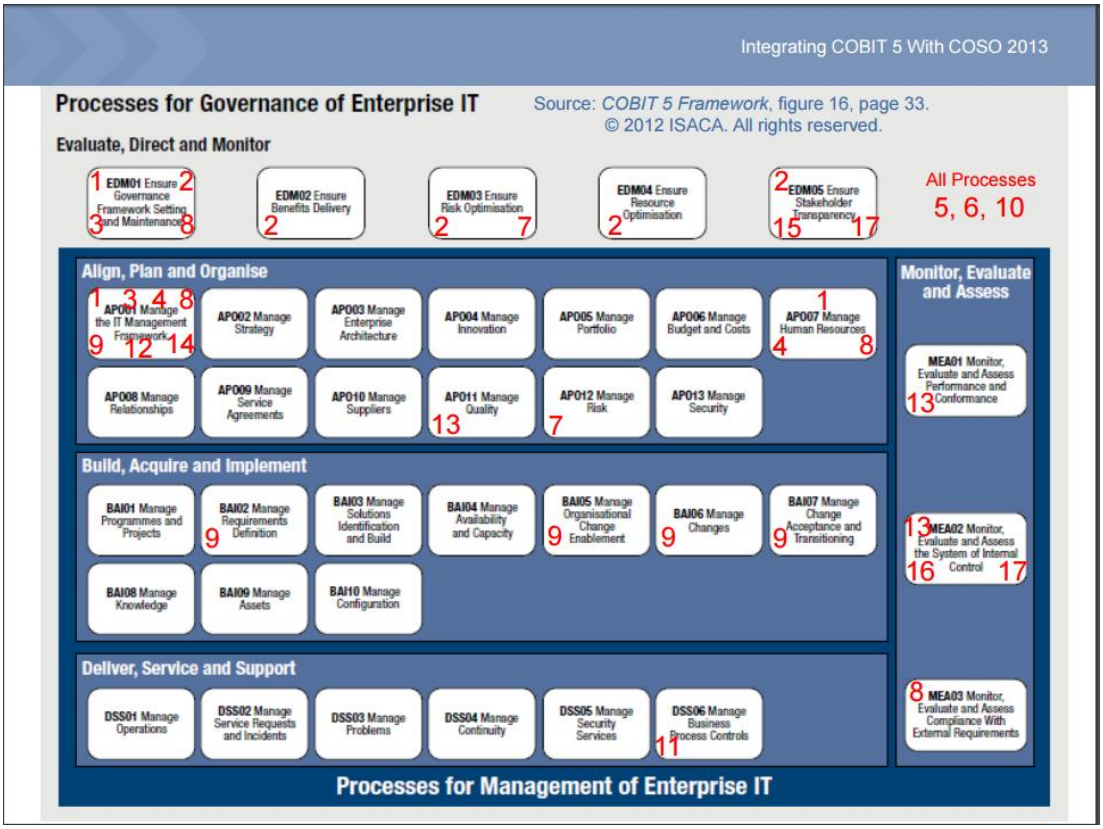
La Administración es la encargada de planificar, construir, ejecutar y monitorear las actividades.

CAPITULO IV

4.1 ESTUDIO COMPARATIVO COBIT 5 COSO III

Para desarrollar las comparaciones de COBIT 5 y COSO III en la gestión de riesgos de información, así como en la gestión de riesgo informático, se basará en el documento llamado "Integrating COBIT 5 With COSO 2013" publicado por (Head, 2014), el mismo que es un resumen del documento publicado por ISACA en el 2014, el cual muestra la relación entre estos modelos y cómo agregan valor a las organizaciones, sin importar la industria o su ubicación geográfica. Esta guía analiza las coincidencias entre COBIT 5 y los 17 principios específicos de COSO, además de mostrar la relación entre el contenido y los conceptos de ambos modelos. (Sánchez, 2015)

GRÁFICO Nº 17: La integración de COBIT 5 y COSO III



Fuente:http://www.isaca.org/chapters3/Charlotte/Events/Documents/Event%20Presentations/10212014/Integrating%20COBIT%205%20With%20COSO.pdf

En la tabla Nº 1 se puede ver claramente la relación existente entre las dos normas, esta tabla permitirá realizar las comparaciones de manera deductiva.

TABLA Nº 1: INTEGRACIÓN O RELACIÓN DE COBIT 5 Y COSO III

17 PRINCIPIOS COSO III	PROCESOS COBIT 5																																						
	EDM01	EDM02	EDM03	EDM04	EDM05	APO01	APO02	APO03	APO04	APO05	APO06	APO07	APO08	APO09	APO10	APO11	APO12	APO13	BAI01	BAI02	BAI03	BAI04	BAI05	BAI06	BAI07	BAI08	BAI09	BAI10	DSS01	DSS02	DSS03	DSS04	DSS05	DSS06	MEA01	MEA02	MEA03
1.- Demuestra compromiso con la integridad y los valores éticos.	*					*						*																										
2.- Ejerce responsabilidad de supervisión.	*	*	*	*	*																																	
3.- Establece estructura, autoridad, y responsabilidad.	*					*																																
4.- Demuestra compromiso para la competencia.						*						*																										
5.- Hace cumplir con la responsabilidad.	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
6.- Especifica objetivos relevantes.	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
7.- Identifica y analiza los riesgos.			*														*																					
8.- Evalúa el riesgo de fraude.	*					*						*																										*
9.- Identifica y analiza cambios importantes.						*														*			*	*	*													
10.- Selecciona y desarrolla actividades de control.	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
11.- Selecciona y desarrolla controles generales sobre tecnología.																																		*				
12.- Se implementa a través de políticas y procedimientos.						*																																
13.- Usa información Relevante.																*																			*	*		
14.- Comunica internamente.						*																																
15.- Comunica externamente.					*																																	
16.- Conduce evaluaciones continuas y/o independientes.		*																																				
17.- Evalúa y comunica deficiencias.					*																															*		

Fuente: Elaborado por el autor.

A continuación se tiene una matriz de detalle de la comparación de COSO III y COBIT5, basado en relación realizada de estas dos normas por ISACA en el año 2014; para lo cual se tomara como base los 17 principios de COSO III y se relacionará con los puntos de COBIT 5.

Tabla Nº 2: COMPARACIÓN DE COSOIII Y COBIT 5

COMPARACIÓN METODOLOGÍAS COSOIII Y COBIT 5		
Actividad/Procesos.	**COSOIII**	**COBIT 5**
1.- Demuestra compromiso con la integridad y los valores éticos.	La organización demuestra compromiso con la integridad y los valores éticos.	Este principio abarca el EDM01 que se refiere al aseguramiento, establecimiento y mantenimiento del marco de gobierno. También al APO01 el cual establece mecanismos para la gestión de la información y el uso de TI. Por último se relaciona con el APO07 que define sobre la gestión de recurso humano estableciendo las funciones y responsabilidades.
2.- Ejerce responsabilidad de supervisión.	El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.	Este punto abarca todos los EDM de COBIT5 que es Evaluar - Dirigir - Monitorear. EDM01 asegura, establece y mantiene al marco de gobierno. EDM02 asegura la entrega de beneficios a la empresa a través de la inversión realizada en los recursos de TI. EDM03 asegura la optimización de riesgo relacionados al uso de TI. EDM04 asegura la disponibilidad y optimización de recursos de TI. EDM05 asegura la transparencia del uso de TI hacia las partes interesadas
3.- Establece estructura, autoridad, y responsabilidad.	La dirección establece, con la supervisión del consejo, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.	Este principio se relaciona con el EDM01 que se refiere al aseguramiento, establecimiento y mantenimiento del marco de gobierno y al APO01 el cual establece mecanismos para la gestión de la información y el uso de TI.

4.- Demuestra compromiso para la competencia.	La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en alineación con los objetivos de la organización	Este punto abarca al APO01 el cual establece mecanismos para la gestión de la información y el uso de TI. También al APO07 que define la gestión de recurso humano estableciendo las funciones y responsabilidades.
5.- Hace cumplir con la responsabilidad.	La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.	Este principio abarca todos los procesos de COBIT5.
6.- Especifica objetivos relevantes.	La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.	Este punto abarca todos los procesos de COBIT5.
7.- Identifica y analiza los riesgos.	La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determinar cómo se deben gestionar.	Este principio abarca el EDM03 el cual permite asegurar la optimización de riesgo relacionados al uso de TI. Así mismo al APO12 que estable la forma de identificar, evaluar y reducir los riesgos relacionados con TI de forma continua.
8.- Evalúa el riesgo de fraude.	La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.	Este punto abarca el EDM01 que se refiere al aseguramiento, establecimiento y mantenimiento del marco de gobierno. También al APO01 el cual establece mecanismos para la gestión de la información y el uso de TI. Así mismo al APO07 que define sobre la gestión de recurso humano estableciendo las funciones y responsabilidades. Por último con el MEA03 que permite Monitorear, Evaluar y Valorar el cumplimiento de los requisitos regulatorios relacionados al área de TI, en conformidad con los Requerimientos Externos.

9.- Identifica y analiza cambios importantes.	La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.	Este principio abarca al APO01 el mismo que establece mecanismos para la gestión de la información y el uso de TI. Así mismo al BAI02 que permite la gestión y definición de requisitos, que satisfagan los requerimientos estratégicos de la empresa antes de su adquisición o creación, BAI05 gestiona la facilitación del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI, BAI06 gestiona todos los cambios de una forma controlada, ya sean cambios de estándares, de mantenimiento de los procesos de negocio, aplicaciones e infraestructura, mediante un análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación. Por último abarca al BAI07 que gestiona la aceptación del cambio y la transición relacionada al área de TI.
10.- Selecciona y desarrolla actividades de control.	La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.	Este principio abarca todos los procesos de COBIT5.
11.- Selecciona y desarrolla controles generales sobre tecnología.	La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.	Este punto se relaciona con el proceso DSS06 de COBIT5, el mismo que gestionar controles de proceso de negocio, definiendo y manteniendo controles apropiados de proceso de negocio, asegurando que la información de la organización satisface todos los requerimientos relevantes.
12.- Se implementa a través de políticas y procedimientos.	La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas a la práctica.	Este principio abarca al APO01 el mismo que establece mecanismos para la gestión de la información y el uso de TI, con el fin de apoyar los objetivos de gobierno de TI en relación con las políticas y los principios rectores.

13.- Usa información Relevante.	La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.	Este punto abarca el APO11 que permite gestionar la calidad en todos los procesos de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia, MEA01 que permite recolectar, validar y evaluar métricas y objetivos de negocio de TI y de supervisar que los procesos se están realizando acorde al rendimiento acordado, por último al MEA02 que permite monitorizar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes, facilitando la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora.
14.- Comunica internamente.	La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.	Este principio abarca al APO01 el mismo que establece mecanismos para la gestión de la información y el uso de TI, con el fin de apoyar los objetivos de gobierno de TI en relación con las políticas y los principios rectores.
15.- Comunica externamente.	15. La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.	Este punto abarca el EDM05 que asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa sean transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.
16.- Conduce evaluaciones continuas y/o independientes.	La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.	Este principio se relaciona con el MEA02 que permite monitorizar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes, facilitando la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora.

17.- Evalúa y comunica deficiencias.	La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda.	Este punto abarca el EDM05 que asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa sean transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias. También se relaciona con el MEA02 que permite monitorizar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes, facilitando la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora.

Fuente: Elaborado por el autor.

Como se puede observar en la Tabla Nº 2 tanto COSO III y COBIT 5, se integran de manera natural, para llevar una gestión optima de la organización; es decir COSO que engloba a todas las áreas de la organización y COBIT 5 que es una guía que permite la administración de una de las áreas más importantes de una empresa que es la de TI.

Es decir al aplicar estas dos normas se puede asegurar que la gestión de riesgos de la información se puede fortalecer a lo máximo, a través de la identificación, evaluación mitigación de los riesgos, analizándolos de forma global e incluyendo a todas las personas que pertenecen a ese contexto.

En el transcurso del desarrollo de la investigación se puede observar que COBIT 5 es una norma que permite la gestión de riesgo informático que engloba a la gestión de riesgo de la información.

4.2 Comparación COBIT 5 y COSO III en la gestión de riesgo informático

La gestión de riesgo informático se relaciona con el área de Tecnologías de la información, el mismo que abarca a la gestión de riesgo de la información, es decir con la utilización de la metodología COBIT 5 que reúne las mejores prácticas para el control y gobierno efectivo de TI, junto con la metodología COSO III que permite

administrar el control interno de una organización; se puede asegurar que la empresa puede alcanzar los objetivos propuestos de manera eficaz; mediante el aseguramiento de una buena gestión de los riegos informáticos.

CAPÍTULO V

CONCLUSIÓNES DE LA INVESTIGACIÓN

COSO III y COBIT 5 son dos metodologías o marcos de referencias que reúnen las mejores prácticas para una buenas gestión empresarias, y estas se pueden complementar para fortalecer y maximizar el control de riesgos a nivel de tecnologías de la información, alineándose con los objetivos de la organización; la alineación y utilización de estas dos normas de puede asegurar que las empresas tengan un sólido marco de referencia para mejorar el proceso del control interno gestionando los riesgos de manera oportuna, incluyendo al área de TI como uno de las áreas base para la correcta administración y gestión de riesgos, todo esto procurando que los objetivos y necesidades del negocio sean cubiertas en el menor tiempo.

Las normas ISO se ha ido evolucionando y mejorando, con el fin de obtener guías óptimas para el buen manejo y administración de las empresas, de esta manera también la construcción de COBIT5 se realiza en base a otros estándares y marcos de referencia, reuniendo de ellos las mejores características, con el fin de obtener una norma robusta adaptable a cualquier tipo de organización sea pequeña, mediana o grande. Este desarrollo se realizó por varios expertos que pertenecen a la fuerza de trabajo de ISACA, en el transcurso del desarrollo se han ido puliendo y mejorando las normas en base a sus experiencias y criterios.

Se puede afirmar que COSO también parte de otros estándares a partir de ellas se ha obtenido una guía que contiene las mejores prácticas para erradicar los riesgos, fraudes, así como orientar a las organizaciones y gobiernos a llevar un control interno eficaz de los procesos que se realizar dentro de la institución. Esta norma al igual que otras ha ido evolucionando y mejorando, la versión actual tiene el nombre de COSO III; el mismo que tiene 17 principios para la creación del Informe COSO, el cual

permite establecer un modelo común de control interno con el cual las organizaciones pueden evaluar sus sistemas de control; esta norma engloba a todas las áreas de la empresa, en cambio la mayoría de las normas ISO son destinadas a un área específica; por ejemplo la norma ISO 31000 es una norma internacional para la Gestión de Riesgos, el cual proporciona principios y una guía que ayuda a las organizaciones a realizar un análisis, evaluación y gestión de riesgos con el fin de mitigar los mismos; de la misma forma la ISO 27001 describe las mejores prácticas para gestionar la seguridad de la información en una empresa.

En definitiva COSO III y COBIT 5 se pueden utilizar de manera complementaria, con el fin de fortalecer la administración interna y gestión de riesgos de TI con el objetivo de guiar a la empresa hacia el éxito.

BIBLIOGRAFÍA

27001 Academy. (s.f.). *¿Qué es norma ISO 27001?* Recuperado el 15 de 01 de 2016, de http://advisera.com/27001academy/es/que-es-iso-27001/

ABS Quality Evaluations. (s.f.). *SISTEMA DE GESTIÓN DE LA INFORMACIÓN*. Recuperado el 07 de 01 de 2016, de http://www.abs-qe.com/es/sistemas-de-gestion-de-la-informacion.html

Amon, J. (2012). *COBIT 5 Procesos Catalizadores*. Estados Unidos: Rolling Meadows. doi:978-1-60420-285-4

Asociación Española para la Calidad. (25 de 03 de 2013). *COSO*. Recuperado el 08 de 04 de 2016, de http://www.aec.es/web/guest/centro-conocimiento/coso

Asociacion Española para la Calidad. (5 de 01 de 2016). *Seguridad de la Información*. Obtenido de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

AUDITOOL. (05 de 2013). *MODELO COSO III - MARCO INTEGRADO DE CONTROL INTERNO*. Recuperado el 18 de 01 de 2016, de http://www.cicinacional.com/images/Articulos/Guia_Marco_Integrado_de_Control_Interno_COSO_III.pdf

Auditool. (05 de 2013). *MODELO COSO III - MARCO INTEGRADO DE CONTROL INTERNO* . Obtenido de www.auditool.org

Barrios, D. (s.f.). *Gestión del conocimiento*. Recuperado el 16 de 01 de 2016, de https://gesconocimientodbd.wordpress.com/gestion-de-la-informacion/

Davis, G., & Olsón. (s.f.). *Gestión de la Información*. Recuperado el 16 de 01 de 2016, de http://www.ecured.cu/Gesti%C3%B3n_de_la_Informaci%C3%B3n

Definición.de. (s.f.). *Definición de riesgo*. Recuperado el 25 de 01 de 2016, de http://definicion.de/riesgo/

Duale, M. (29 de Juilo de 2013). *El riesgo de la información: 10 lecciones extraídas de la experiencia de las propias empresas*. Recuperado el 20 de 01 de 2016, de http://www.revistacloudcomputing.com/2013/07/el-riesgo-de-la-informacion-10-lecciones-extraidas-de-la-experiencia-de-las-propias-empresas/#sthash.pkVs7CX9.dpuf

González, M. (1998). *Sistemas de Gestión de Información*. Recuperado el 17 de 01 de 2016, de http://www.ecured.cu/Gesti%C3%B3n_de_la_Informaci%C3%B3n

Gutiérrez, C. (12 de 12 de 2013). *ISO/IEC 27002:2013 y los cambios en los dominios de control*. Recuperado el 16 de 01 de 2016, de http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

Head, S. (2014). *Integrating COBIT 5 With COSO 2013*. Recuperado el 22 de 02 de 2016, de http://www.isaca.org/chapters3/Charlotte/Events/Documents/Event%20Presentations/10212014/Integrating%20COBIT%205%20With%20COSO.pdf

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid: ISACA® Framework. doi:978-1-60420-282-3

ISO. (26 de 01 de 2016). *ISO 31000: 2009.* Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=43170

ISO 27001 en Español. (3 de 01 de 2016). *¿Qué es un SGSI?* Obtenido de http://www.iso27000.es/sgsi.html

ISO 27002.es. (23 de 01 de 2016). *LOS CONTROLES DE ISO/IEC 27002*. Obtenido de El portal de ISO 27002 en Español: http://www.iso27000.es/iso27002.html

ISO Tools exelence. (05 de 10 de 2015). *Cómo implantar eficazmente la norma ISO 27005*. Recuperado el 20 de 01 de 2016, de https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/

Maxitana, J., & Naranjo, B. (2005). *Administración de riesgos de tecnología de información de una empresa del sector informático*. Recuperado el 20 de 02 de 2016, de https://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen%20Cicyt.-%20Administraci%C3%B3n%20de%20Riesgos%20de%20TI%20de%20una%20empresa%20del%20sector%20Inform%C3%A1tico.pdf

Mejía, R. (2008). Administración de riesgos. Un enfoque empresarial. Universidad EAFIT. doi:9588281237

Morales, D. (24 de 02 de 2012). Diseño de un modelo de gestión administrativo financiero para las pymes dedicadas a las actividades comerciales en la ciudad de Quito. En D. C. Morales Muñoz. Quito: Universidad Politécnica Salesiana Ecuador. Recuperado el 13 de 01 de 2016, de http://dspace.ups.edu.ec/handle/123456789/1442

Posada Moreno, G. (01 de 03 de 2007). *Calidad ¿Ques es la ISO?* Obtenido de http://www.degerencia.com/articulo/calidad_que_es_la_iso

Ramírez, A. (04 de 09 de 2012). *Riesgo tecnológico y su impacto para las organizaciones parte I*. Recuperado el 06 de 02 de 2016, de

http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

Ritegno, E. O. (2012). *Gestión de Riesgos de TI*. Buenos Aires: Banco de la Nación Argentina.

Rodiguez, I. (19 de 09 de 2015). *¿Qué es el riesgo, riesgo inherente y riesgo residual?* Recuperado el 05 de 02 de 2016, de http://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

Sánchez, E. (08 de 2015). *Control Interno y COSO*. Recuperado el 23 de 02 de 2016, de http://www.isaca.org/chapters4/Mexico-City/Documents/CONTROL%20INTERNO%20Y%20COSO.pdf

Sperat, S. (s.f.). *Todo lo que usted quería saber sobre COBIT 5 y no se animó a preguntar*. (B. Galiotti, Editor) Recuperado el 08 de 01 de 2016, de http://estratega.org/todo-lo-que-usted-queria-saber-sobre-cobit-5-y-no-se-animo-a-preguntar/

SRI. (s.f.). *¿Qué son las PYMES?* Recuperado el 14 de 01 de 2016, de http://www.sri.gob.ec/de/32

taringa.net. (2011). *Informe COSO - Control Interno en Organizaciones*. Obtenido de http://www.taringa.net/post/economia-negocios/5884893/Informe-COSO---Control-Interno-en-Organizaciones.html

Universidad Abierta a Distancia UNAD - Colombia. (3 de 01 de 2016). *Ciclo PDCA (Edward Deming)*. Obtenido de Sistema de Gestion de la Seguridad de la Informacion SGSI: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

White. (s.f.). *Gestión de la Información*. Recuperado el 15 de 01 de 2016, de http://www.ecured.cu/Gesti%C3%B3n_de_la_Informaci%C3%B3n

Woodman, L. (s.f.). *Gestión de la Información*. Recuperado el 15 de 01 de 2016, de http://www.ecured.cu/Gesti%C3%B3n_de_la_Informaci%C3%B3n

ANEXOS:

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay,

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 05 de noviembre de 2015, conoció la petición del (los) estudiante(s) **Pablo Andrés Minchala Márquez** con código(s) **46484**, registrado(s) en la Unidad de Titulación Especial, quien(es) denuncia(n) su trabajo de titulación denominado: **"ESTUDIO COMPARATIVO DE LAS METODOLOGIAS COBIT 5 Y COSO III PARA LA GESTION DEL RIESGO DE TI"**en la modalidad: Proyecto de investigación y presentado como requisito previo a la obtención del título de Ingeniero de Sistemas y Telemática .-El Consejo de Facultad acoge el informe de la Junta Académica y aprueba la denuncia. Designa como Director(a) a Ing. Esteban Crespo Martínez y como miembro del Tribunal Examinador a Ing. Francisco Salgado Arteaga. De conformidad con el cronograma de la Unidad de Titulación el (los) peticionario(s) debe presentar su trabajo de titulación hasta el 11 de marzo de 2016.

Cuenca, 06 de noviembre de 2015

Dra. Jenny Ríos Coello
Secretaria de la Facultad de Ciencias de la Administración

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACIÓN
SECRETARÍA

Oficio Nro. 170-2015-DIST-UDA

Cuenca, 4 de noviembre de 2015

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 4 de noviembre del 2015, recibió el proyecto de tesis titulado "Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI", presentado por el estudiante Pablo Andrés Minchala Márquez estudiantes de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ing. Esteban Crespo Martínez, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior a al Ing. Esteban Crespo Martínez y como miembro del Tribunal a Francisco Salgado Ph.D.

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

CONVOCATORIA

Por disposición de la Junta Académica de Administración de Empresas, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: ***"Estudio comparativo de las metodologías COBIT 5 Y COSO III para la gestión del riesgo de TI"***, presentado por el estudiante **Minchala Márquez Pablo Andrés**, con código **46484**, previa a la obtención del grado de Ingeniero en Sistemas y Telemática, para el día **MIERCOLES, 04 DE NOVIEMBRE DE 2015 A LAS 08:30 AM.**

Cuenca, 30 de octubre de 2015

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Esteban Crespo Martínez .....

Ing. Francisco Salgado Arteaga .....

UNIVERSIDAD DEL AZUAY

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** Pablo Andrés Minchala Márquez
Código: 46484
1.2 **Director sugerido:** Ing. Esteban Crespo Martínez
1.3 **Codirector (opcional):** _____
1.4 **Tribunal:** Ing. Francisco Salgado Arteaga
1.5 **Título propuesto: (proyecto de investigación)** *"Estudio comparativo de las metodologías COBIT5 y COSO III para la gestión del riesgo de TI".*
1.6 **Resolución:**

1.6.1 Aceptado sin modificaciones ✓

1.6.2 Aceptado con las siguientes modificaciones:

_____

_____

_____

1.6.3 Responsable de dar seguimiento a las modificaciones:
1.6.4 No aceptado
- Justificación:

_____
_____
_____

Tribunal

Ing. Esteban Crespo Martínez

Ing. Francisco Salgado Arteaga

Sr. Pablo Minchala Márquez

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: miércoles 04 de noviembre de 2015 a las 08:30 am.

1. Protocolo/Rúbrica

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Minchala Márquez Pablo Andrés
Código 46484
1.2 Director sugerido: Ing. Esteban Crespo Martínez
1.3 Codirector (opcional):
1.4 Título propuesto: (proyecto de investigación) *"Estudio comparativo de las metodologías COBIT5 Y COSO III para la gestión del riesgo de TI".*
1.5 Revisores (tribunal): Ing. Francisco Salgado Arteaga
1.6
1.7 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?	✓			
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?				
11.¿Es factible de verificación?				
Objetivo general				
12.¿Concuerda con el problema formulado?	✓			

13.¿Se encuentra redactado en tiempo verbal infinitivo?	✓			
Objetivos específicos				
14.¿Concuerdan con el objetivo general?	✓			
15.¿Son comprobables cualitativa o cuantitativamente?	✓			
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?	✓			
17.¿Las actividades se presentan siguiendo una secuencia lógica?	✓			
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?	✓			
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	✓			
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?	✓			
21.¿Concuerdan con los objetivos específicos?	✓			
22.¿Se detalla la forma de presentación de los resultados?	✓			
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	✓			
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?	✓			
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	✓			
Presupuesto				
26.¿El presupuesto es razonable?	✓			
27.¿Se consideran los rubros más relevantes?	✓			
Cronograma				
28.¿Los plazos para las actividades son realistas?	✓			
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?	✓			
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?	✓			

1. Protocolo/Rúbrica

31.¿El texto se encuentra libre de faltas ortográficas?	/			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

Ing. Esteban Crespo Martínez

Ing. Francisco Salgado Arteaga

UNIVERSIDAD DEL AZUAY

Cuenca, 4 de Noviembre del 2015

Señor Ingeniero

Xavier Ortega Vázquez

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINNISTRACIÓN

Presente.-

De mis consideraciones:

Yo Pablo Andrés Minchala Márquez con código 46484 solicito a usted que me conceda la aprobación del proyecto de titulación con el tema "Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI" que aportara en el campo de investigación.

Por la atención que preste a la presente anticipo mis agradecimientos.

Atentamente,

Pablo Andrés Minchala Márquez

46484

CI: 0104032339

Edición autorizada de 30.000 ejemplares
Del 708.501 al 738.500 Nº 0715793

UNIVERSIDAD DEL AZUAY

Universidad del Azuay

Facultad de Administración

Escuela de Ingeniería de Sistemas y Telemática

"Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI"

Trabajo de graduación previo a la obtención del título de:

"Ingeniero en Sistemas y Telemática"

Autor:

Pablo Andrés Minchala Márquez.

Director:

Ing. Paul Esteban Crespo Martínez.

Cuenca, Ecuador

2015

Edición autorizada de 30.000 ejemplares Nº 0715800
Del 708.501 al 738.500

Universidad del Azuay

Ingeniería de Sistemas y Telemática
Metodología de la Investigación

Guía para la presentación de la propuesta de proyecto de titulación

1. Datos generales

1.1 Nombre del estudiante: Minchala Márquez Pablo Andrés.
1.1.1 Código: 46484
1.1.2 Contacto: 0742137141, 0996582622
minchalapablom@hotmail.com

1.2 Director sugerido: Crespo Martínez Paul Esteban Ing.
1.2.1 Contacto: ecrespo@uazuay.edu.ec

1.4 Asesor metodológico: Ninguno.

1.5 Tribunal designado:

1.6 Aprobación:

1.7 Línea de Investigación de la carrera:
Informática de computadores
Sistemas de Seguridad de la Información.

1.7.1 Código UNESCO

Código UNESCO: **1203**

1.7.2 Tipo de trabajo:
Investigación formativa

1.8 Área de estudio: Seguridad de la Información.

1.9 Título propuesto: "Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI".

1.10 Estado del proyecto: La propuesta realizará un estudio comparativo entre las metodología COBIT 5 y COSO III, y su vinculación con las normativas 27001, 27002, 27005, y 31000, utilizadas para el análisis y gestión de riesgos de seguridad de la información. Este estudio se inserta en la línea propuesta en el proyecto de investigación de seguridad de la información que propone la escuela de Ingeniería de Sistemas y Telemática: "Desarrollo de una metodología para el análisis y gestión de riesgo informático en las empresas del sector MPYME ecuatoriano".

2. Contenido

2.1 Motivación de la investigación:

Actualmente todas las micro, pequeñas y medianas empresas (MPYME) no tienen claro el concepto, ni el alcance con el que cuenta la gestión de riesgos, por lo tanto, no adoptan las buenas prácticas para el correcto manejo de esta área integrador

Con este fin, se ha planteado realizar una investigación y evaluación de las normativas existentes en la actualidad y que se puedan aplicar a las MPYME para realizar una correcta y adecuada gestión de riesgos.

2.2 Problemática:

No existe una normativa definida y cien por ciento aplicable a micro, pequeñas y medianas empresas (MPYME) en lo que a gestión de riesgos se refiere. Por lo tanto, estas perciben a las normativas COSO, COBIT y las ISO como algo demasiado extenso y complejo para ser aplicable en sus organizaciones.

2.3 Resumen:

Este trabajo pretender realizar un análisis comparativo de las metodologías COBIT 5 y COSO III, utilizadas para la gestión de riesgos de información; con el objetivo de aportar a la construcción de una metodología para la gestión de riesgos informáticos, en el ámbito de empresas y organizaciones del sector MPYME Ecuatoriano.

Edicion autorizada de 30.000 ejemplares Del 708.501 al 738.500 Nº 0715799

2.4 Indagación exploratoria y base conceptual:

¿Qué es un riesgo informático?

Un riesgo hace referencia a la incertidumbre o probabilidad de que ocurra una eventualidad, la misma que puede estar prevista, un riesgo es la posibilidad de que exista un daño.

Un riesgo informático se refiere a la incertidumbre o probabilidad que ocurra un suceso con amenaza creíble de daño respecto a bienes o servicios informáticos entre los que se pueden mencionar: equipos hardware y sus periféricos, instalaciones, proyectos, programas software, archivos, información o datos confidenciales con los que cuenta una organización. (Audisistemas, 2009)

¿Qué es COBIT?

Control Objectives for Information and related Technology o su significado en español: Objetivos de control para la información y tecnologías relacionadas, es una guía de mejores prácticas que es presentada como un modelo marco, y que está dirigida al control y supervisión de la tecnología de información (TI).

COBIT cuenta con una serie de recursos que pueden servir de modelo de referencia para la adecuada gestión de TI:

- Modelo marco (*Framework*)
- Descripción de procesos
- Objetivos de control
- Directrices de gestión
- Modelos de madurez

Desde 1996 se han publicado varias ediciones siendo las más importantes:

UNIVERSIDAD DEL AZUAY

- COBIT 4.1 (2007): contiene 34 procesos que cubren 210 objetivos de control que se los clasifica en cuatro dominios:
  1. Planificación y Organización
  2. Adquisición e Implementación
  3. Entrega y Soporte
  4. Supervisión y Evaluación
- COBIT 5 (Abril 2012): está basado en COBIT 4.1, y se lo amplía mediante la integración a otros *frameworks* y normas como son: *Val IT, Risk IT, Information Technology Infrastructure Library* (ITIL) y las normas ISO relacionadas a estas normas.
- COBIT para la seguridad de la información: es básicamente una guía práctica para el mejoramiento de la seguridad de la empresa; mediante su uso e implementación, ayuda a las empresas a reducir el riesgo mediante la adecuada administración de la seguridad. (ISACA)

¿Qué es COSO?

Committee of Sponsoring Organizations of the Treadway Commission o Comité de Organizaciones Patrocinadoras de la Comisión *Treadway*, es una iniciativa conjunta de cinco organizaciones del sector privado de Estados Unidos, que se dedican a proporcionar liderazgo a través de la elaboración de marcos y orientación sobre la correcta gestión del riesgo empresarial (ERM), el control interno y evitar el fraude.

Las organizaciones que la conforman son:

- La Asociación Americana de Contabilidad (AAA)
- El Instituto Americano de Contadores Públicos Certificados (AICPA)
- Ejecutivos de Finanzas Internacional (FEI)
- el Instituto de Auditores Internos (IIA)
- La Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [AMI]).

Edición autorizada de 30.000 ejemplares
Del 708.501 al 738.500 Nº 0715798

COSO estudia los factores que pueden generar información fraudulenta dentro de las organizaciones, elabora textos y recomendaciones para ser utilizados por todo tipo de organizaciones y entidades reguladoras. Se lo puede encontrar como modelo COSO; en cuanto a la gestión de riesgos existen los informes COSO I y II y en mayo del 2013 se publicó la tercera versión COSO III, siendo esta ultima la versión a analizar. (Ladino, 2009)

¿Qué son las MPYME?

Mejor conocidas como micro, pequeñas y medianas empresas; son empresas con características definidas en cuanto a límites ocupacionales y financieros, que han sido determinadas por los diferentes estados o regiones en donde han sido creadas.

Generalmente están limitadas en cuanto a capital, inversiones, número de empleados y volumen de ventas; ya que cuando las MPYME superan los umbrales determinados que las clasifican como tales, pasan a clasificarse como grandes empresas. (SRI, 2015) (Bedford, 2010)

- Microempresas: emplean hasta 9 trabajadores, tienen ingresos de hasta 100 mil dólares y un valor de activos no superior a 100 mil dólares. (Zapata, 2015)
- Pequeña Empresa: puede tener hasta 49 trabajadores, ingresos con un rango entre 100 mil y 1 millón de dólares, y sus activos se encuentran en el rango entre 100 mil a 750 mil dólares. (Zapata, 2015)
- Mediana Empresa: emplean de 50 a 199 trabajadores, sus ingresos no sobrepasan los 5 millones de dólares, sus

UNIVERSIDAD DEL AZUAY

activos se encuentran en el rango entre 750 mil a 4 millones de dólares. (Zapata, 2015)

- Grandes Empresas: son aquellas que tienen más de 200 trabajadores, sus ingresos son superiores a 5 millones de dólares y sus activos se encuentran en un valor superior a 4 millones de dólares. (Zapata, 2015)

2.5 Objetivo general:

Realizar un análisis comparativo entre las metodologías COBIT 5 Y COSO III utilizadas en el análisis y gestión de riesgo informático.

2.6 Objetivos específicos:

- Argumentar teóricamente la gestión de riesgos de información y la gestión de riesgo informático.
- Estudiar la metodología COBIT 5 y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000
- Estudiar la metodología COSO III y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000
- Comparar las metodologías COSO III y COBIT 5 en el ámbito de la gestión de riesgo de información y riesgo informático.

2.7 Metodología:

Para el desarrollo del proyecto se realizará una revisión e investigación de las normativas y los marcos de referencia antes mencionados y adicionalmente se podrá realizar un análisis de estudios realizados por terceros. Este proceso se realizará con el fin de recopilar la información necesaria, y tener un conocimiento a profundidad de las normativas y la realidad actual respecto a las MPYME en el Ecuador.

Edición autorizada de 30.000 ejemplares Del 708.501 al 738.500 Nº 0715797

2.8 Alcances y resultados esperados:

El proyecto pretende generar un documento de la comparativa de las metodologías COBIT 5 y COSO III en base a mecanismos para la gestión del riesgo de información, identificación de activos y vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo, y su alineación con la familia ISO 27000 e ISO 31000; a fin de poder determinar cuál de ellas es la más viable a utilizar por las MPYME, en el contexto del proyecto de investigación de la Universidad del Azuay.

2.9 Supuestos y riesgos:

Falta de información.- en caso de no poder tener acceso a las documentación de las metodologías COBIT 5 y COSO III debido al alto costo de las mismas.

2.10 Presupuesto:

Rubro-Denominación	**Costo USD (detalle)**	**Justificación ¿para qué?**
Internet	$100	El uso de internet dentro de este proyecto es primordial ya que mediante este se puede obtener toda la información necesaria
Impresiones	$100	Que servirán para entregar los documentos físicos del proyecto a realizarse
Equipos y Suministros	$0	Debido a que los equipos utilizados dentro del proyecto son propiedad del único integrante del proyecto (Pablo Andrés Minchala Márquez)
Gastos Varios	$50	En los que se incluye transportación e imprevistos que puedan presentarse dentro del proyecto

2.11 Financiamiento:

El financiamiento con el que se contará para la realización de este proyecto de fin de carrera y que ha sido

UNIVERSIDAD DEL AZUAY

desglosado en el presupuesto general, será cubierto en su totalidad por el autor (Pablo Andrés Minchala Márquez).

2.12 Esquema tentativo

PORTADA

DEDICATORIA

AGRADECIMIENTOS

ABSTRACT

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

OBJETIVO GENERAL

OBJETIVOS ESPECÍFICOS

JUSTIFICACIÓN

CAPÍTULO 1 - MARCO TEÓRICO

- ¿Qué es riesgo informático?
- ¿Qué es COSO III?
- ¿Qué es COBIT 5?
- ¿Qué son las normas ISOS?
- ¿Qué son las MPYME?

CAPÍTULO 2 – Análisis de la Gestión de Riesgos de TI – COSO III

CAPITULO 3 – Análisis de la Gestión de Riesgos de TI – COBIT 5

CAPITULO 4 – RESULTADOS

- Cuadro comparativo entre las metodologías COSO III y COBIT 5

CONCLUSIONES

RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

Edición autorizada de 30.000 ejemplares
Del 708.501 al 738.500
Nº 0715796

2.13 Cronograma:

Objetivo Específico	Actividad	Resultado esperado	Tiempo (semanas)
Argumentar teóricamente la gestión de riesgos de información y la gestión de riesgo informático.	Revisión de documentación y conceptos a utilizarse dentro del desarrollo del proyecto	Marco teórico completo	2 semanas
Estudiar la metodología COSO III y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000	Análisis de información respecto a Gestión de Riesgos de TI de acuerdo a la metodología COSO III	Cuadro de resultados referentes a Gestión de Riesgos de TI de la normativa COSO III	6 semanas
Estudiar la metodología COBIT 5 y determinar su alineación con las normativas ISO 27001, 27002, 27005 y 31000	Análisis de información respecto a Gestión de Riesgos de TI de acuerdo a la metodología COBIT 5	Cuadro de resultados referentes a Gestión de Riesgos de TI de la normativa COBIT 5	6 semanas
• Comparar las metodologías COSO III y COBIT 5 en el ámbito de la gestión de riesgo de información y riesgo informático	Realizar un cuadro comparativo entre las metodologías COBIT 5 y COSO III	Cuadro comparativo entre las metodologías COBIT 5 y COSO III	4 semanas

UNIVERSIDAD DEL AZUAY

2.14 Referencias:

AEC. (Mayo de 2013). *AEC - COSO.* Obtenido de http://www.aec.es/web/guest/centro-conocimiento/coso

Audisistemas. (2009). *Audisistemas - Riesgos Informáticos.* Obtenido de http://audisistemas2009.galeon.com/productos2229079.html

Bedford, R. (Diciembre de 2010). *12. Resolucion SUPER CIAS PYMES - SC-INPA-UA-G-10-005.pdf.* Obtenido de http://www.russellbedford.com.ec/images/Boletines%202010/12.%20Resolucion%20SUPER%20CIAS%20PYMES%20-%20SC-INPA-UA-G-10-005.pdf

ISACA. (s.f.). *COBIT Objetivos de control para la información y tecnologías.* Recuperado el 5 de Septiembre de 2015, de http://es.ccm.net/contents/596-cobit-objetivos-de-control-para-la-informacion-y-tecnologias-re

Ladino, E. (2009). Control interno: informe Coso. Obtenido de http://site.ebrary.com/lib/uasuaysp/detail.action?docID=10317346&p00=coso

SRI. (2015). *Pymes - Servicio de Rentas Internas.* Obtenido de http://www.sri.gob.ec/de/32

Téllez, J. (1988). *Capitulo III - Riesgos Informáticos.* Obtenido de http://biblio.juridicas.unam.mx/libros/2/909/5.pdf

Zapata, J. E. (10 de Octubre de 2015). Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/1442/5/Capitul

2.15 Anexos:

Edición autorizada de 30.000 ejemplares Del 708.501 al 738.500 Nº 0715795

2.16 Firma de responsabilidad (estudiante)

Pablo Minchala

Pablo Andrés Minchala Márquez

2.17 Firma de responsabilidad (director sugerido)

Ing. Paul Esteban Crespo Martínez

2.18 Fecha de entrega

4 de noviembre de 2015