MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

# Modelo integrado de gestión de riesgos de seguridad en los departamentos de TIC

**Propuesta de artículo presentado como requisito para la obtención del título:**

**Magíster en Auditoría de Tecnologías de la Información**


**Por el estudiante:**
**Cristhian Yuri Romero Romero**

**Bajo la dirección de:**
**Ing. Oiner Gómez Baryolo (PhD.)**

**Universidad Espíritu Santo**
**Maestría en Auditoría de Tecnología de la Información**
**Samborondón - Ecuador**



**Abril 2017**

# *Modelo integrado de gestión de riesgos de seguridad en los departamentos de TIC*

Cristhian Yuri Romero Romero[1]

Resumen

En el presente trabajo se analizaron las normas que constituyen la base para el desarrollo de un modelo de gestión, seleccionando las más idóneas según sus características de adaptabilidad en los departamentos de Tecnologías de la Información y Comunicación (TIC), aplicable a cualquier organización pública o privada. Para la revisión de la información, se consideraron los aspectos más relevantes en cuanto a los procesos generales que competen a las normativas ITIL, ISO 9001, 31000, 27005, 17799, COBIT. Entre las partes analizadas obtenidas de la revisión de fuentes bibliográficas se encuentran: el alcance, el contexto organizacional, el soporte y la mejora para la organización. Una vez establecidas las ventajas que proporcionan las normativas analizadas, se escogieron las normas y características más relevantes para la elaboración del modelo de gestión de riesgos y su validación. Como resultado se obtuvo que las normativas ISO 9001, 27005 y 31000 presentaron características adaptables y aplicables a un modelo integrado de gestión de riesgos, que se ajusta a los requerimientos de las TIC, así como los procesos y activos de la información relacionados con ellas; adicionalmente se aplicó el modelo a la Fiscalía General de El Oro con la finalidad de validar el mismo. En el análisis se determinó que la organización tiene un nivel de cumplimiento del modelo propuesto de un 59%. Los resultados de la aplicación de esta norma dependieron de la organización en la que se ejecuta la empresa. Se puede constatar que una de las partes más importantes para la adecuada gestión de los riesgos de seguridad, la constituyen las revisiones periódicas y documentadas que contemplen los apropiados medios de comunicación interna.

Palabras clave: ISO, Modelo de Gestión, Seguridad de la Información, Riesgos.

Abstract

In the present work the rules that constitute the basis for the development of a management model were analyzed, selecting the most suitable ones according to their characteristics of adaptability in the Departments of Information and Communication Technologies (ICT), applicable to any public organization or Private. For the review of the information, the most relevant aspects were considered regarding the general processes that correspond to the ITIL, ISO 9001, 31000, 27005, 17799, COBIT standards. Among the analyzed parts obtained from the revision of bibliographic sources are: the scope, the organizational context, the support and the improvement for the organization. Once the advantages provided by the regulations analyzed were established, the most relevant norms and characteristics were chosen for the elaboration of the risk management model and its validation. As a result, the ISO 9001, 27005 and 31000 standards presented adaptable and applicable characteristics to an integrated risk management model, which is in line with the requirements of ICT, as well as the processes and information assets related to them; Additionally, the model was applied to the Attorney General of El Oro with the purpose of validating the same. In the analysis it was determined that the organization has a level of compliance of the proposed model of 59%. The results of the application of this standard depended on the organization in which the company is run. It can be verified that one of the most important parts for the proper management of the security risks is the periodic and documented revisions that contemplate the appropriate means of internal communication.

Key words ISO, Management Model, Information Security, Risk.

[1] Estudiante de la Maestría en Auditoria de Tecnologías de la Información Universidad Espíritu Santo – Guayaquil - Ecuador- E-mail cristhianromero@uees.edu.ec.

## INTRODUCCIÓN

Las Tecnologías de la Información y Comunicación (TIC) en las organizaciones constituyen una herramienta importante de apoyo a la gestión empresarial, para conocer su implementación se requiere de un proceso complejo que involucra múltiples dimensiones en aspectos técnicos, legales y sociales. A partir de esta apreciación, se puede definir a las TIC, como elementos facilitadores del manejo de la información. Así mismo, se considera que su adecuada aplicación, puede proporcionar ventajas competitivas para las empresas o instituciones que lo implementan (Carr, 2012).

Con base a esta perspectiva, las empresas que consideran necesaria la implementación de sistemas de gestión integrados dentro de su modelo de trabajo, deben regirse a diversas normas internacionales que sirven de guía para asegurar que los estándares de calidad y seguridad se cumplan, con la ayuda de la aplicación y adaptación de las especificaciones técnicas establecidas en las diferentes normas internacionales vigentes.

En este contexto, dentro de las normativas más representativas a nivel internacional, se pueden mencionar las siguientes; Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), así como también la Organización Internacional para la Estandarización (ISO) ha creado normativas relacionadas con la gestión de la calidad, tales como la norma ISO 9001, manejo del riesgo ISO 31000, gestión de riesgos de la seguridad de la información ISO/IEC 27005 e ISO 17799 (Núñez, 2012).

La Organización Internacional de Estandarización (ISO), ha desarrollado y establecido normas cuya aplicación es de carácter voluntario; las cuales en la actualidad se han convertido en parte de los requisitos para que una organización ingrese al sector productivo o de servicios, puesto que se exponen las directrices para el mejoramiento de la calidad en diferentes campos, entre los que se encuentra el manejo de las herramientas tecnológicas a nivel empresarial (Mezquida, 2011).

En este caso, las normas enfocadas a gestionar las TIC están concertadas principalmente en el COBIT e ITIL. Actualmente, en diversos países a nivel mundial, un importante número de empresas han implementado sistemas de gestión para detectar a tiempo problemas relacionados con la calidad de los servicios que se ofertan dentro de las plataformas informáticas, ya sea del sector público o privado. A pesar de que la mayor parte de estos sistemas cuentan con herramientas para facilitar la gestión de procesos relevantes a nivel operativo, no todas las empresas toman en consideración la implementación de sistemas de gestión de riesgo de seguridad informática dentro de los departamentos de TIC (United Nations Publications, 2012).

De acuerdo a los resultados expuestos, en diversos artículos científicos, las principales falencias que se suelen presentar en relación a los sistemas que gestionan los riesgos de seguridad de TIC, radican principalmente en el manejo del sistema y los recursos. Es por esto que la modificación se centra generalmente en el mejoramiento de los procesos desde un enfoque de calidad, dejando de lado la gestión de riesgos de seguridad informática.

La identificación de las falencias en los sistemas de seguridad con relación al manejo de la información en los departamentos de TIC, precisa que los directivos y personal administrativo tomen decisiones sobre las acciones que se deben ejecutar para mejorar la calidad de gestión, considerando la medida en que las normativas internacionales establecidas en el COBIT e ITIL, permiten mitigar las deficiencias de sus sistemas actuales.

Para las empresas que utilizan las TIC en la gestión de la información de sus procesos, se ha evidenciado que la principal deficiencia en sistemas de gestión integrados se encuentra en la incapacidad de gestionar los riesgos de seguridad de información. En la mayoría de las organizaciones se suelen presentar riesgos físicos y tecnológicos como elementos aislados, restándole importancia al impacto que causan en conjunto, ya que pueden influir en la

productividad de las organizaciones. (Suárez, 2015).

Con base a los antecedentes expuestos, los departamentos de TIC se exponen a riesgos de seguridad, y presentan falta de precisión en la manera en que se maneja la información, a esto se suman los riesgos físicos a los que están expuestos los modelos de gestión que existen en las organizaciones, los cuales permiten su correcto funcionamiento. Por esta razón resulta necesario asegurar la integridad, confidencialidad y disponibilidad de la información.

En el Ecuador las empresas se encuentran expuestas a ataques informáticos en los sistemas que manejan dentro de sus organizaciones, además de problemas asociados al uso de los recursos físicos, como es el caso de Fiscalía General de El Oro, en la que de acuerdo a una auditoría previamente realizada se identificaron los siguientes riesgos en el departamento de TIC: Errores en el sistema utilizado, asociados principalmente a la corrupción de los datos; la exposición a malware, que afecta el correcto funcionamiento de los equipos informáticos; la propagación de virus entre ordenadores, atribuido a la descarga de información o apertura de correos maliciosos; el procesamiento de datos incorrectos, eliminación de datos descuidados, o la apertura accidental de archivos adjuntos de correos electrónicos infectados; y amenazas informáticas relacionadas con el robo de información confidencial.

Esto puede preverse y corregirse mediante la aplicación de medidas que protegen la información que se gestiona en el departamento de TIC y la seguridad de los medios físicos. Por lo tanto, el objetivo del presente estudio se basa en analizar de forma comparativa las principales normas y estándares existentes, con la finalidad de seleccionar las normas que puedan adaptarse a cualquier tipo de organización. Considerando que su aplicación permitirá establecer una base para el diseño de un modelo integrado de gestión de riesgos de seguridad, que contribuya a la protección y gestión adecuada de la información de los departamentos de TIC y los medios físicos de las organizaciones públicas o privadas.

## MARCO TEÓRICO

### *Tecnologías de la información.*

Las TIC han tenido un papel importante en la sociedad, ya que se encuentran inmersas en las actividades diarias de los individuos y las organizaciones; por lo general principalmente en la educación, robótica y las actividades empresariales. Son importantes ya que se trata de los recursos, herramientas o programas que sirven para administrar información a través de soportes tecnológicos como computadoras, dispositivos móviles, reproductores de audio y televisores (Cabero, 2012).

Las TIC facilitan el acceso a la información de manera rápida y en cualquier formato. Entre las características que tienen se destacan las siguientes: Digitalización de la información, es decir que se podrá contar con esta en cualquier momento, particularmente en pequeños soportes que almacenen mucha información; permiten la comunicación birrelacional entre personas sin importar donde se encuentren, principalmente mediante el uso de video conferencias, mensajería instantánea u otros sistemas. Varios procesos se han automatizados con la implementación de las TIC, esto ha contribuido a mejorar la vida de muchas personas, con ordenadores que programan actividades que se ejecutan automáticamente (Sales, 2014).

Según lo manifiesta Katz (2012), "Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos informáticos y de telecomunicaciones. De forma general se puede decir que las nuevas TIC, son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones" (p. 34).

### *Ventajas y desventajas de las TIC.*

Las principales ventajas que proporcionan las TIC son:

1. Permiten el fácil acceso, almacenamiento y procesamiento de información.
2. Reducen el tiempo en las operaciones que se ejecuten con el manejo de la información.

3. Contribuye al incremento de los índices de eficiencia en los departamentos administrativos de las empresas.

Entre las desventajas se encuentran las siguientes:

1. Perdida de información cuando existen errores en el sistema.
2. Escasa capacitación en el manejo de equipos tecnológicos.
3. Los usuarios no están adaptados a los servicios tecnológicos (Arrarte, 2011).

***Definición de riesgo.***

Según lo menciona Téllez (2011), "El riesgo se refiere a la incertidumbre o probabilidad de que ocurra una eventualidad, la cual puede estar prevista; en este sentido podemos decir que el riesgo es la contingencia de un daño" (p. 33).

Las normas ISO definen el riesgo como la probabilidad de que se suscite algún tipo de amenaza, utilizando vulnerabilidades que existen en un activo o grupo de activos, lo que puede provocar daños o pérdidas en una organización o empresa.

***Gestión del riesgo***

Para Fernández (2012), "La gestión de riesgo se encuentra definido como el proceso en el cual se puede identificar, analizar y cuantificar cuáles son las probabilidades de pérdidas y efectos secundarios que se pueden provocar de los desastres que ocurran, también permite que se establezcan acciones preventivas, correctivas y reductivas que deben tomarse" (p. 23).

Las organizaciones, sin importar las dimensiones de trabajo, se encuentran expuestas a la influencia de factores internos tales como: comunicación, estructura, capital; y externos, como las fluctuaciones del mercado, la competencia, entre otros. Estos aspectos afectar la posibilidad de alcanzar los objetivos propuestos, por lo tanto, se perciben como un riesgo, el cual debe ser gestionado.

***Normativas, modelos y estándares para la gestión del riesgo en TIC.***

Actualmente, existen diversos modelos de gestión de riesgos, que se orientan a los sistemas de las TIC, para proteger la información digital con la que cuentan las empresas públicas y privadas; estas normativas están basadas en los requerimientos que poseen las organizaciones. Por lo tanto, en las siguientes secciones se analizarán las normas que guardan relación con la gestión de riesgo en las TIC.

***COBIT 5.***

Según lo referencia ISACA (2011), "Este es un sistema de control estándar desarrollado como un organismo que se centra en temas de gobernabilidad, control y aseguramiento de auditorías para las TIC" (p. 45).

COBIT 5, se trata de un modelo para auditar y gestionar los sistemas de control de información y tecnología, se encuentra orientado a todos los sectores de las organizaciones, es decir, está dirigido a administradores, auditores y usuarios que se encuentran inmersos en los procesos. Dentro de este, se monitorea y controlan los negocios y la seguridad informática y lo que abarque el control específico (Brand & Boonen, 2014).

Este sistema de información puede ser aplicado a cualquier empresa, en computadoras personales o de redes. Se basa en que los recursos tecnológicos deben ser administrados por procesos que brinden información confiable para que una organización o empresa pueda cumplir sus objetivos planteados (Vanegas & Murillo, 2014).

Para Bernard (2012), "La misión de COBIT se basa en buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información generalmente aceptada, para usarse de forma diaria por gestores de negocio y auditores" (p. 12).

El COBIT 5 es un sistema de control muy amplio debido a que puede aplicarse en todos los departamentos, es decir que no es una norma especializada en el control de seguridad de riesgos informáticos, razón por la cual no puede ser tomado en cuenta como base para el diseño de un modelo integrado de gestión de

riesgos en el departamento de TIC. (Encalada Loja & Cordero Guzmán, 2016)

***Principios de COBIT 5.***

Entre los principios de COBIT 5 se encuentran los siguientes: Cumplir con las necesidades de los interesados, mantener a la organización de manera integral, implementar un solo marco integral, permitir un enfoque holístico y distinguir el gobierno de la administración.

Este sistema esta enfocado principalmente en los procesos de control, teniendo prioridad la ejecucion de las actividades que realiza una organización. No obstante, este modelo no considera todos los aspectos que integran a un sistema de gestion optimo, tales como: calidad, servicio y seguridad. Así mismo, otra dificultad radica en que para implementar estos principios, se considera prioritariamente la planificación estratégica diseñada por los directivos de la organización y no puede ser delegada a otros departamentos (ISACA, 2014).

***ITIL.***

Para Baker (2011), "Es una norma desarrollada pensando en la implementación de mejores prácticas para la administración de servicios de tecnologías de información" (p. 27).

La Biblioteca de Infraestructura de Tecnologías de Información, es un conjunto de buenas prácticas que son utilizadas en la gestión de servicios de TIC. ITIL permite establecer instrucciones detalladas de los procedimientos de gestión que se utilizan para que las organizaciones puedan alcanzar la calidad y eficiencia esperada de las operaciones de las TIC. Estos procedimientos se encuentran aislados del proveedor y son diseñados como guía para la infraestructura y desarrollo de las operaciones tecnológicas (Office of Government Commerce, 2012).

Sin embargo, esta no es una metodología de desarrollo de software que hace enfoque a sistemas que aún no han sido desarrollados, ITIL ofrece métodos de control que permiten mejorar los servicios o productos que están en etapa de madurez.

En este contexto, se puede decir que estos procedimientos están en una etapa de mejora continua y todos giran en torno a la estrategia de servicios de transición, operación y diseño.

No obstante, una de las principales dificultades que suelen suscitarse bajo la aplicación de esta norma, radica en la gran cantidad de tiempo que se requiere para su introducción de las organizaciones, ya que suele ocurrir que no se cumplen los objetivos. La limitante que tiene en relación a la gestión de riesgos, se basa en que no cuenta con las herramientas de soporte adecuadas para permitir la mejora de procesos (Bon & Jong, 2012).

***LEY SOX.***

El SOX, es una abreviatura para Sarbanes Oxley Act la cual es una ley que fue emitida en el año 2002 en Estados Unidos, para poder contrarrestar los diversos escándalos financieros que se produjeron en relación a falsificación de información financiera, lo que obligo a las empresas a buscar estrategias de seguridad que protejan los procesos de dicha información, para esto elaboraron sistemas de protección de información (International Labour Organization, 2012).

Entre las principales limitantes de este sistema, se destaca la necesidad de que el programa sea instalado por una persona especializada y capacitada en relación al sistema. El objetivo principal que tiene este sistema de gestión, se centra en monitorear el área financiera para sancionar a los ejecutivos que estén cometiendo fraudes. Por lo que las empresas que cuentan con este modelo tienen mayor confiabilidad en los informes que emiten (Fonseca, 2012).

***ISO 27005.***

Es un estándar internacional que se encarga de gestionar riesgos de información. La norma proporciona directrices de seguridad para gestionar los riesgos de seguridad informática en empresas, esta norma se apoya en la ISO 27001 donde se encuentran los requisitos de información definidos. Puede ser aplicada a varios tipos de organizaciones que requieran gestionar riesgos en relación a seguridad informática (Talabi, 2012).

En la actualidad, esta norma se ha convertido en un estándar, ampliamente aplicado en empresas e instituciones privadas o públicas, independientemente del sector empresarial al cual pertenecen. Cuenta con anexos que tienen ejemplos e intereses para los usuarios, en estos anexos se pueden ver las amenazas tabuladas, al igual que vulnerabilidades que están relacionadas con los activos de la información.

Las fases de aplicación de esta norma son las siguientes: Establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, y monitorización y revisión del riesgo.

De acuerdo a los antecedentes de aplicación, se puede constituir como una de las mejores metodologías ya que no da paso a la incertidumbre. Sin embargo, se trata de una abstracción y un nivel elevado en el que no está detallado o describe los riesgos (Corletti, 2011).

***ISO 31000.***

Según lo menciona Myburgh (2012), "Proporciona directrices genéricas sobre la gestión del riesgo, permitiéndole al igual que las normativas ISO 9001 y 27005 ser aplicables a cualquier empresa. Este nuevo estándar, provee un marco de trabajo (Framework) en su estructura, y un proceso que se encuentra destinado a gestionar cualquier tipo de riesgo de forma transparente, sistemática y creíble, dentro de cualquier alcance o contexto" (p. 76).

El propósito de esta norma es proporcionar principios para la gestión de riesgos, ayudar a las organizaciones en el análisis y evaluación de la gestión de riesgos. Esta norma contribuye a mejorar las técnicas de gestión de seguridad en el lugar de trabajo, permite que se optimice la eficacia operativa y consecuentemente establece la confianza en las partes interesadas y reduce las pérdidas.

***Ventajas de la ISO 31000.***

Las principales ventajas del uso de esta norma son: Produce confianza entre las partes interesadas en relación al uso de técnicas de riesgos, permite aplicar controles de sistemas de gestión para reducir los daños y pérdidas, mejora la eficacia operativa, permite que se den cambios rápidos de forma eficaz y protege a la empresa en el proceso de crecimiento.

Entre los limitantes de la norma ISO 31000 se destacan los siguientes: No da garantía de que se identifiquen todas las zonas de riesgo, y tampoco determina la forma en que se organiza las medidas de riesgo.

***ISO 9001.***

La última versión de la normativa ISO es la ISO 9001:2015, la cual fue desarrollada considerando que la tecnología y la forma de trabajar han cambiado, lo que ha dado lugar a que se incremente la complejidad en la cadena de suministro. Consecuentemente, para que la norma ISO 9001 pueda seguir aplicándose de forma óptima, se realizaron adaptaciones al sector empresarial. Esta norma se aplica para las gestiones de calidad de los elementos de administración y ha contribuido significativamente con las empresas para asegurar que se satisfagan las necesidades de los clientes y se cumplan con los requisitos legales (Vértice, 2012).

Los 10 principios de la gestión de calidad con la que cuenta son:

1. Orientación al cliente y satisfacción del mismo.
2. Liderazgos.
3. Participación de los involucrados.
4. Centra su enfoque en los procesos.
5. Gestión de sistemas.
6. Procura la mejora continua.
7. Permite tomar decisiones.
8. Relación de beneficio mutuo con los proveedores.
9. Permite entregar un mejor servicio o producto al cliente.
10. Mejora los procesos de planificación y comunicación.

En la norma ISO 9001 se establecen los requisitos estandarizados para el funcionamiento adecuado de los sistemas de calidad, por esta razón es considerada como líder en relación a sistemas de gestión de calidad. De su aplicación se derivan los siguientes beneficios: incremento de la cuota

de mercado, reducción de costes y el aumento de efectividad en la gestión de riesgo.

***ISO 17799.***

Propone un conjunto de controles que sirven de guía para realizar una revisión detallada de la situación de los sistemas en cuanto a la seguridad. La norma ISO/IEC 17799 es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado.

Esta norma, define un conjunto muy amplio de controles de seguridad. Sin embargo, no ofrece una solución global al problema de la seguridad porque carece de mecanismos de gestión (Calder, 2012).

***Tendencias actuales en sistemas de gestión de riesgos informáticos.***

Con el objetivo de llevar a cabo correctamente los procesos de auditoría y desarrollar procesos óptimos que cumplan estándares de seguridad y calidad se implementan las evaluaciones de las TIC o modelos de gestión de riesgo, dentro de las organizaciones. Para esto efecto, en la actualidad se diseñan controles que abordan los aspectos relacionados con el área de la información.

Las nuevas tendencias se encuentran encaminadas a la integración de sistemas de gestión, dando a conocer los nuevos retos que están relacionados al análisis de las normativas en función de los requisitos de aplicación en las empresas. Las organización en la actualidad tienen gran interés en incorporar un sistema de gestión de riesgo que avale la aplicación de estándares de calidad y seguridad para que las operaciones en el departamento de TIC se manejen de forma óptima (Aguilera, 2011).

***Ciclo Planificar, Hacer, Verificar Actuar (PHVA)***

Según lo define Vergara (2011):

> Considerando las condiciones cambiantes dentro del entorno empresarial, es importante que toda empresa prestadora de servicios este en capacidad de darle una solución a los problemas que se presenten, en este sentido el ciclo PHVA se constituye en una herramienta efectiva para tal efecto (p. 64).

Para desarrollar este ciclo se requieren de los siguientes pasos:

1. Establecer el problema.
2. Analizar el problema.
3. Determinar las causas fundamentales del problema.
4. Realizar un plan de acción para contrarrestar las causas del problema.
5. Verificar que se contrarresten los problemas.
6. Estandarización para prever la reaparición de los problemas.
7. Estudiar la solución del problema.

El uso de forma continua del PHVA permite que se encuentre una solución que se mantenga la competitividad de los productos y servicios que ofrece una empresa, para mejorar la calidad, reducir costos y mejorar de forma continua la productividad, disminuir precios, aumentar la participación de mercados.

***Planificar***

Estas acciones son preventivas: Definir las metas y establecer métodos para cumplir las metas. Dentro de esta fase se establecen los objetivos y los procesos que se realizaran para poder obtener resultados en relación a los requerimientos del cliente y las políticas que se manejan en la organización.

Para esto se realizan los siguientes pasos:

1. Identificar el servicio y los clientes.
2. Determinar requerimientos de los clientes.
3. Diagramar los pasos claves del proceso.
4. Establecer la capacidad del proceso.
5. Realizar el benchmarks.

***Hacer***

Se refiere a las acciones de ejecución: Realizar el trabajo. En esta fase se establece las oportunidades de mejora, se desarrolla un plan piloto y se implementan estas mejoras.

***Verificar***

Son acciones de evaluación: Comprobar los resultados de las tareas que se ejecutaron. Aquí se realiza un seguimiento y se miden los procesos de los servicios y las políticas, además de los requisitos del producto para poder conocer sobre los resultados.

***Actuar***

Se toman acciones correctivas: Eliminar no conformidades detectadas. Se toman las acciones de mejoramiento continuo para desarrollar procesos, aquí se implementa lo que fue definido en la planeación y es alienado a toda la organización, se forman equipos de trabajo y son documentados en los procesos que tienen enfoque de PHVA y con una metodología definida.

**Comparativo de las normas de seguridad de información**

A partir de la información documental previamente analizada, a continuación, se resume los aspectos más significativos de cada uno de los indicadores. Con relación al alcance, en lo que respecta a la normativa se pueden observar clausulas sobre las directrices de la gestión de riesgos, en aspectos de planificación, auditoría interna y externa, y las mediciones. En el contexto organizacional se puede establecer y analizar la organización monitoreando las situaciones de riesgo.

El análisis del soporte indica que para la implementación las normas ISO 9001, ISO 27005 e ISO 31000 son compatibles con el ciclo PHVA. Ya que proporcionan estándares para evaluación, políticas, valoración y tratamiento de riesgos tecnológicos. También presentan mejoras para la organización con estándares de mejoramiento de calidad, gestión de riesgo y seguridad del manejo de información.

El grupo de normas ISO tiene un estándar formal, que es aplicado según la norma utilizada de la misma forma las normativas analizadas en este trabajo tienen una estructura esquemática particular, por lo que no son aplicables en todas las situaciones. Se presenta un cuadro comparativo de las normas analizadas en el anexo 1.

## METODOLOGÍA

La metodología bajo la cual se basó el estudio previo, consistió en el diseño y aplicación de la investigación mixta, es decir cuali - cuantitativa, la misma que fue de utilidad para recabar información primaria mediante la técnica de la entrevista y la encuesta. Según Ruiz (2012), la técnica de la entrevista consiste en una conversación entre dos personas, y se efectúa de una manera formal.

El instrumento de investigación que se aplicó fue el guion de preguntas, el cual se diseñó previamente con preguntas abiertas, lo que permitió obtener información a profundidad sobre el objeto de estudio por parte de los entrevistados (Yuni & Urbano, 2014). Se aplicó además la técnica de la encuesta, utilizando como instrumento un cuestionario con la finalidad de comprobar si se cumplió con el objetivo propuesto y todas las normas inmersas en el mismo (Heinemann, 2012).

En relación al análisis de los resultados que se obtuvieron mediante la encuesta estos se representarán mediante porcentajes a través de la comprobación de madurez, la misma que es una herramienta diseñada para que los directivos de la organización (sin tener conocimientos específicos de las normas ISO), puedan realizar de una forma rápida una evaluación del sistema de gestión de riesgo (Ramón, 2010); de tal forma se debe mencionar que la finalidad de esta actividad es el obtener respuestas a través de las opiniones de los involucrados (Ildefonso, 2011).

El tipo de investigación que se determinó a aplicar fue la descriptiva, la cual según Mas (2010), permite tener información a profundidad sobre un hecho en particular, esto a través de la exploración de los fenómenos en la vida real ofreciendo una descripción

detallada de las características de ciertas situaciones, por ello, a través de este tipo de investigación fue posible identificar como podría contribuir un modelo integrado de gestión de riesgos de seguridad en los departamentos TIC.

Se consideró importante aplicar a su vez el método analítico, el cual según Bernal (2012) consiste en el análisis de un objeto en particular, partiendo de la relación que existen entre los elementos que conforman dicho objeto como un todo, a su vez, la síntesis se produce sobre la base de los resultados.

En lo que respecta a los análisis, estos se demostraron a través de un comparativo dentro del marco teórico, a fin de identificar cuáles son las normas más idóneas a ser utilizadas dentro del modelo integrado de gestión de riesgo de seguridad, de acuerdo a este resultado se realizó el alineamiento PHVA el mismo que incluyó a las 3 normas ISO en conjunto, presentando la aplicación mediante una tabla. (Ver anexo 2)

## ALINEACIÓN PHVA CON EL MODELO INTEGRADO DE GESTIÓN DE RIESGO

La alineación PHVA, se realizó en base a cuatro fases identificadas como; Planear, Hacer, Verificar y Actuar. El cual brinda una solución que permite mantener la competitividad de los servicios, mejorando la calidad, la productividad, reduciendo costos, aumentando la rentabilidad de la empresa. (Bustamante, 2012)

De la misma forma se analizaron las normas ISO 27005, 31000, 9001. Estas dieron como resultado que las mismas son compatibles con el método PHVA, en la cual se identificó que en lo que respecta a las fases:

Identificación, esta fase se alinea con la etapa Planear del modelo PHVA, se utiliza la cláusula comprender la organización y su contexto que se encuentra en la norma ISO 9001, mientras que con la norma ISO 31000 se procede a diseñar el marco en el que se trabaja la gestión de riesgo y con la ISO 27005 se determina la secuencia e interacción de los procesos de la valoración del riesgo, dichas cláusulas permitirán el análisis del contexto organizacional, conocer mecanismos de comunicación, procesos y procedimientos de la gestión de riesgos dentro de la organización.

La fase aplicación se alinea con la etapa Hacer, se establece las políticas para la gestión de riesgo con la ISO 31000, se implementa el plan de tratamiento con la norma ISO 27005, seguido del cambio de diseño y desarrollo con la ISO 9001, estas normas se enfocan en realizar actividades e implementar soluciones que permitan a la organización monitorear, responder y recuperarse de una interrupción en los servicios.

En lo que respecta al control, se realiza el monitoreo y revisión de los factores de riesgo con la ISO 27005, el monitoreo y revisión del marco de referencia con la ISO 31000, y con la norma ISO 9001 se efectúa el seguimiento, medición, análisis y evaluación, esta fase se alinea con la etapa Verificar y ejecutará la revisión y evaluación del desempeño de la capacidad de respuesta y recuperación de un riesgo tecnológico.

Se finaliza con la Mejora, la cual se alinea con la fase actuar, y se realiza mediante la revisión y mejora para la gestión de riesgo con la ISO 27005, seguido de la mejora continua con las normas ISO 9001 y 31000, dichas normas dirigen la implementación de acciones correctivas que mejorarán el desempeño del sistema de gestión de riesgos.

A continuación, se presenta una descripción de cada una de las fases y actividades propuestas en el modelo (Figura 1).

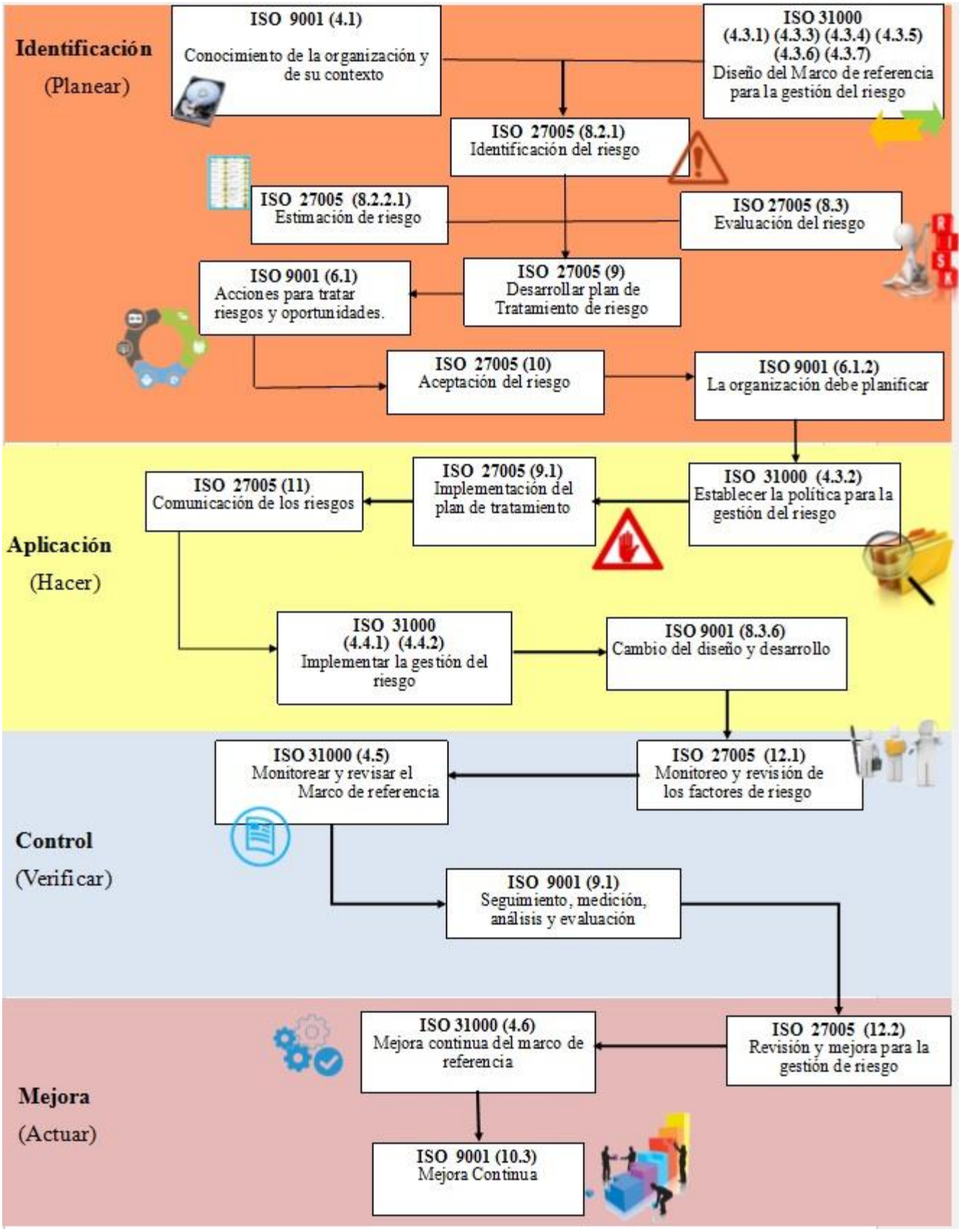


*Figura 1.* Modelo Integrado de Gestión de Riesgo de la Seguridad alineado con las fases Planificar, Hacer, Verificar, Actuar, mediante las normas ISO 9001, 31000, 27005.

## PROCEDIMIENTO

La recolección de información se efectuó de forma presencial a través del desarrollo de la entrevista, la misma que fue realizada al encargado del departamento de TIC de la Fiscalía General de El Oro identificada como empresa pública y al jefe de la empresa privada Holcim.

Recalcando que para la aplicación del modelo se realizó en una entidad pública, esto se debe por la facilidad que proporcionó al momento de generar la recaudación de información y por el corto tiempo que existe, lo que hace que no se pueda aplicar en las dos organizaciones.

En otro apartado, en lo que respecta a la comprobación de la efectividad del modelo de gestión de riesgo, se procedió a realizar mediante un cuestionario cuya calificación permitió identificar el nivel de madurez y el grado de cumplimiento de los sub componentes de las normas ISO 27005, 31000, 9001, el mismo que identifica la aprobación de la gestión de seguridad como solución para empresas que generen los mismos inconvenientes encontrados en la investigación.

## ANÁLISIS RESULTADOS

De acuerdo a la realización de las entrevistas en ambas empresas pública y privada, se proporcionó la siguiente información:

*Tabla 1* Entrevista realizada a las empresas Holcim y Fiscalía provincial de El Oro

| PREGUNTAS | RESPUESTAS | |
|---|---|---|
| | HOLCIM | FISCALÍA |
| **Rol dentro del departamento TIC.** | Planificar, organizar, dirigir y controlar sistemas informáticos. Y mantenimiento óptimo de sistemas de redes y equipos de cómputo. | Soporte a los servicios de redes y equipos informáticos y administrar las cuentas de Usuarios en el Sistema SIAF 1.0 Y 2.0. |
| **Procesamiento de la información.** | Mediante el correo empresarial https://departamento .tic@holcim.com. | Mediante el correo (https://mail.fiscalia. gob.ec) cuya planta central es Quito. |
| **Problemas más críticos.** | Fallas de red, hardware y software. | Fallas de red, hardware y software, reseteo de las cuentas de usuarios de la plataforma de la Fiscalía. |
| **¿Cuenta con un modelo de gestión de riesgo?** | Actualmente no, ya que el último modelo de gestión se dio de baja. | No, alguna inconveniente se lleva de manera empírica. |
| **Soluciones a problemas.** | Se presenta un informe al gerente general de la empresa y se soluciona con la ayuda de expertos del área. | Se presenta un reporte si se soluciona o no, se procede a informar a Planta Central. |
| **Norma de calidad y seguridad que conoce.** | Han sido capacitados sobre la norma ISO 9001 ya que la empresa la usa. | Desconoce. |
| **¿Por qué se debe implementar un modelo de gestión de riesgo?** | Porque se registrará mediante un modelo de gestión las posibles soluciones que la empresa requiera. | Porque reducirá los tiempos de respuesta de los soportes de Hardware y Software y se mejorará la calidad de los servicios a nivel técnico. |

Con la intención de identificar riesgos y vulnerabilidades de seguridad en los departamentos de TIC se aplicó el modelo de gestión de riesgos mediante una encuesta a la Fiscalía General de El Oro.

La evaluación del modelo planteado fue cuantificada mediante ponderaciones que consideraron 5 rangos, con una asignación de grado de cumplimiento. (Ver anexo 3). Obteniendo como resultados, un nivel de madurez y un porcentaje de cumplimiento de las normas (Ver anexo 4), que se detalla a continuación.

Como resultado general, se encontró un grado de compatibilidad del 59% para la actual gestión de riesgos de seguridad en el departamento de TIC de la Fiscalía General de El Oro (Ver tabla 1), según el modelo propuesto en la presente investigación, donde se puede visualizar que en el consolidado de los componentes: identificación, aplicación, control y mejora se alcanza una valoración de 3, en un nivel de madurez Manejado (Ver figura 2), de acuerdo al siguiente detalle:

En la etapa de identificación se obtiene un 56% de cumplimiento, porque la organización posee estructura, políticas, objetivos, roles y responsabilidades, activos, sistemas de información, mecanismos de comunicación interna y externa, entre otros; por lo contrario, no elije adecuadas herramientas y técnicas de identificación y tratamiento de riesgos ya que no ha desarrollado un plan de gestión de riesgos y dichas vulnerabilidades las solucionan de manera empírica.

En lo que corresponde al componente aplicación se obtuvo como resultado un porcentaje del 60%, la evaluación refleja la presencia de documentos de intervención de los riesgos, ya que se llevan a cabo el tratamiento y seguimiento de riesgos y vulnerabilidades mediante mecanismos, los mismos que no forman parte de un plan de gestión de riesgos organizacional.

Por lo siguiente se observa la fase de control con un 55% de cumplimiento, debido a que la organización monitorea activos, incidentes de la seguridad de la información y se presentan informes sobre el control de vulnerabilidades, pero no revisa periódicamente si el marco de referencia, la política y la gestión del riesgo son adecuados, según el contexto externo e interno de la organización.

Finalizando con el análisis de los componentes se verifica que el grado de cumplimento de la mejora fue de un 63%, ya que la fiscalía garantiza que los recursos para el tratamiento de riesgos y vulnerabilidades están disponibles continuamente y las actividades relacionadas sean adecuadas en las circunstancias actuales, además en la organización todas las mejoras acordadas para los procesos se notifican a los directores correspondientes, existiendo un bajo nivel en la toma decisiones sobre la forma en que se podrían mejorar el marco de referencia, la política y el plan para la gestión del riesgo, la investigación de las causas del bajo desempeño y para apoyar la mejora continua.(Ver anexo 5)

El resultado de la aplicación del modelo integrado de gestión de riesgos de seguridad, constituye una parte esencial para la toma de decisiones por parte la Fiscalía General de El Oro para el mejoramiento de estos aspectos.

*Tabla 2* Consolidado de la evaluación del Modelo de Gestión de Riesgos

| COMPONENTES | VALORACIÓN | NIVEL DE MADUREZ | % CUMPLIMIENTO |
|---|---|---|---|
| Identificación - Planear | 2,8 | MANEJADO | 56% |
| Aplicación - Hacer | 3,0 | DEFINIDO | 60% |
| Control - Verificar | 2,8 | MANEJADO | 55% |
| Mejorar - Actuar | 3,2 | DEFINIDO | 63% |
| **NIVEL TOTAL DE MADUREZ** | **2,9** | **MANEJADO** | **59%** |

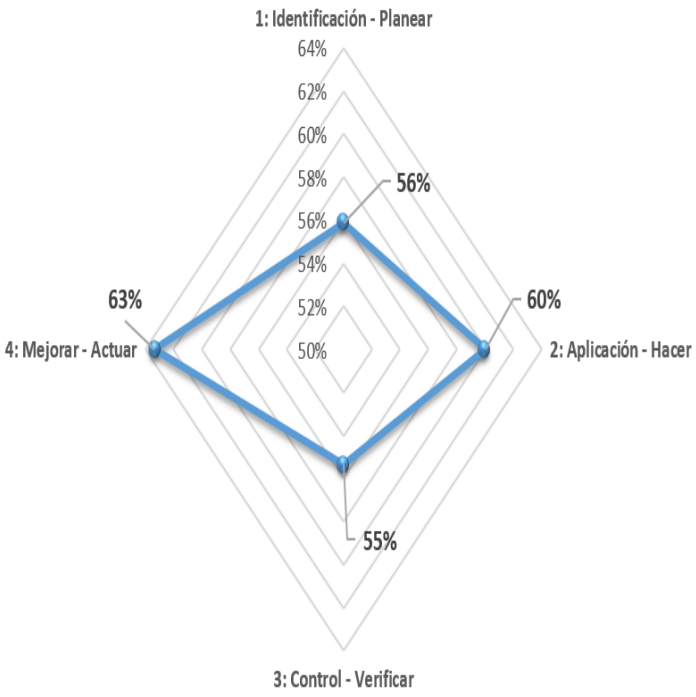


*Figura 2.* Gráfica representativa del nivel de madurez de la Fiscalía de El Oro.

## CONCLUSIONES

Los resultados obtenidos en el trabajo realizado permiten concluir lo siguiente:

Las distintas normativas analizadas en este trabajo tienen una estructura esquemática particular y al comparar las principales características comunes implicadas en la gestión de riesgo las normas ISO 9001, 27005 y 31000 son mayormente compatibles, tomando como parámetros la valoración de los riesgos informáticos y de la infraestructura, evitando los vacíos y ambigüedades que tienen los estándares.

El método PHVA consiste en un enfoque iterativo de cuatro fases que sirven para mejorar continuamente procesos, servicios y resolver problemas, el análisis de las normas ISO 27005, 31000, 9001 demuestra que son compatibles con este ciclo y dichas normativas integradas al modelo propuesto poseen cláusulas sobre las directrices de la gestión de riesgos, en aspectos de contexto organizacional, valoración y tratamiento del riesgo, y mejora.

La identificación de responsabilidades en la implementación y aplicación del modelo de integrado de gestión de riesgos es un elemento fundamental, considerando que el monitoreo de los resultados, constituye una parte esencial para el mejoramiento de las falencias de la organización.

La aplicación del modelo integrado de gestión de riesgos, determinó que la Fiscalía General de El Oro alcanzó un nivel de cumplimiento de un 59% debido a que la organización posee estructura, políticas, objetivos, roles y responsabilidades, diversos activos, sistemas de información, mecanismos de comunicación interna y externa, por lo contrario, no ha desarrollado un plan de gestión de riesgos y las vulnerabilidades las solucionan de manera empírica.

Realizar esta investigación presentó ciertas limitaciones, mismas que se detallan a continuación: La poca accesibilidad a las normas ISO actualizadas ya que las mismas están disponibles en páginas Web oficiales cuya descarga tiene un costo financiero; la aplicación del modelo se realizó en una entidad pública, esto se debe por la facilidad que proporcionó al momento de generar la recaudación de información y por el corto tiempo que existió, lo que hizo que no se pueda aplicar en las dos organizaciones.

El modelo integrado de gestión de riesgos de seguridad en los departamentos de las TIC, tiene una connotación dinámica y por lo tanto está sujeto a nuevas modificaciones según sea el contexto de su implementación. Será necesario que se lleven a cabo estudios posteriores para identificar algún tipo de variación en los resultados de cumplimiento, considerando un período más extenso.

## RECOMENDACIONES

Casi todas las medidas descritas hasta ahora están destinadas a evitar el acceso no autorizado a los sistemas. No obstante, está claro que habrá personas de su entorno que necesiten acceso de alto nivel a los sistemas. Toda estrategia de seguridad será imperfecta a menos que pueda garantizar que estas personas no van a hacer un uso indebido de los derechos que se les han concedido.

Así mismo, para estudios posteriores se recomienda analizar las normativas que se adapten al tipo de empresa o departamento en el cual se busque implementar un modelo integrado de gestión de riesgos de seguridad, así como la evaluación mediante la aplicación de otro tipo de métodos científicos.

De igual manera para futuras investigaciones se debe emplear documentación existente en la organización, entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones y diversas evaluaciones que se consideren necesarias relacionadas con calidad, seguridad, planeación estratégica y continuidad, las mismas que sirvan para la obtención de información que permita certificar a la organización con respecto a su gestión de riesgos tecnológicos.

# BIBLIOGRAFÍA


ISACA . (2011). *COBIT and Application Controls: A Management Guide.* ISACA .

Aguilera, F. (2011). *Seguridad informática.* Editex.

Arrarte, G. (2011). *Las tecnologías de la información en la enseñanza del español.* Arco Libros.

Baker, J. (2011). *Introduction to ITIL.* The Stationery Office.

Bernal, C. (2012). *Métodologia de la investigación.* México: Pearson Educación .

Bernard, P. (2012). *COBIT® 5 - A Management Guide.* Van Haren.

Bon, J. v., & Jong, A. (2012). *Gestión de Servicios TI basado en ITIL® V3 - Guia de Bolsillo.* Van Haren.

Brand, K., & Boonen, H. (2014). *IT Governance: A Pocket Guide Based on COBIT.* The Stationery Office.

Bustamante, R. (2012). *Sistema de gestión integral.* Colombia: Universidad de Antioquia.

Cabero, J. (2012). *Diseño y producción de TIC para la formación.* Editorial UOC.

Calder, A. (2012). *International IT Governance: An Executive Guide to ISO 17799/ISO 27001.* Kogan Page Publishers.

Calder, A. (2013). *The Case for ISO27001:2013.* IT Governance Publishing.

Carr, N. (2012). *Las tecnologías de la información: son realmente una ventaja competitiva?* Empresa Activa.

Corletti, A. (2011). *Seguridad por niveles.* Alejandro Corletti.

Encalada Loja, C., & Cordero Guzmán, D. (2016). GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE COBIT 5: CASO UNIVERSIDAD CATÓLICA DE CUENCA (UCACUE. *Revista Científica y Tecnológica UPSE*, 114-115.

Fernández, A. (2012). *La gestión del riesgo operacional: de la teoría a su aplicación.* Ed. Universidad de Cantabria.

Fonseca, O. (2012). *Sistemas de Control Interno Para Organizaciones.* Paraninfo S.A.

Heinemann, K. (2012). *Intriducción a la metodología de la investigación empírica.* Barcelona: Paidotribo.

Ildefonso, E. (2011). *Fundamentos y técnicas de investigación comercial .* Madrid: Esic Editorial.

International Labour Organization. (2012). *Buen gobierno.* International Labour Organization.

ISACA. (2014). *Controls & Assurance in the Cloud: Using COBIT 5.* ISACA.

Katz, R. (2012). *El Papel de las TIC en el Desarrollo.* Editorial Paraninfo .

Mas Ruiz, F. (2010). *Temas de investigación técnica.* España: Editorial Club Universitario.

Mas, F. (2010). *Temas de investigación técnica.* España: Editorial Club Universitario.

Mezquida, A. C. (2011). Sistema de gestión integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *Revista Española de Innovación, Calidad e Ingeniería del Software, 6*(3), 25-34.

Myburgh, D. (2012). *ISO 31000Rx: the Risk Management Index.* Lulu.com.

Núñez, E. (2012). *Archivos y normas ISO.* Trea.

Office of Government Commerce. (2012). *Introduction to the ITIL service lifecycle.* Office of Government Commerce.

Ramón, J. (2010). *Modelo de madurez para comprobación de gestión de riesgo.* México: Lulu Santos.

Ruiz, J. (2012). *Metodología de la investigación cualitativa .* Bilbao: Universidad de Deusto.

Sales, C. (2014). *El método didáctico a través de las TIC: un estudio de casos en el aulas.* Nau Llibres.

Suárez, C. (2015). *Tecnologías de la Información Y la Comunicación (módulo).* Ideaspropias Editorial S.L.

Talabi, M. (2012). *Information Security Risk Assessment Toolkit.* Newnes.

Téllez, J. (2011). *Contratos, riesgos y seguros informáticos.* UNAM.

United Nations Publications. (2012). *Las tecnologías de la información y la comunicación (TIC).* United Nations Publications.

Vanegas, L., & Murillo, J. (2014). *Auditoria de Sistemas: Estandar Cobit 4.1.* Dreams Magnet.

Vergara, J. (2011). *La gestión de la calidad en los servicio ISO 9001:2008.* Juan C Vergara Schmalbach.

Vértice, E. (2012). *Gestión de la calidad (ISO 9001/2008).* Equipo Vértice.

Watkins, S. (2013). *ISO27001:2013 Assessments Without Tears.* IT Governance Publishing.

Yuni, J., & Urbano, C. (2014). *Técnicas para investigar.* Buenos Aires: Editorial Brujas.

# ANEXOS

## Anexo 1 Tabla comparativa de las normas

| | ISO 9001 | ISO 31000 | ISO 27005 | COBIT 5 | ISO 17799 | ITIL |
|---|---|---|---|---|---|---|
| ALCANCE | Promueve el enfoque basado en procesos y añade el concepto del pensamiento basado en riesgo, está orientada a mejorar la calidad de atención mediante el complimiento de objetivos claves. | Garantiza la aplicación de un sistema eficaz para la gestión de riesgos siendo aplicable a cualquier tipo de organización. | Aporta directrices para establecer una adecuada gestión de riesgo de la información y es aplicable a todo tipo de organización. | Propone un marco de acción el cual evalúa los criterios de información como la seguridad y calidad además de auditar recursos que comprenden las TIC. | Propone un conjunto de controles que sirven de guía para realizar una revisión detallada de la situación de los sistemas en cuanto a seguridad. | Proporciona a los administradores de sistemas de TIC las herramientas y documentos que les permiten mejorar la calidad del servicio que ofertan. |
| REFERENCIA NORMATIVA | Cláusulas 4.1, 4.2 4.4, hacen referencia a la reducción de efectos indeseados<br>Las cláusulas 6.1, 7.5 hacen referencia a la necesidad de abordar riesgos mediante planificación. | Aporta las directrices para una auditoría interna y externa del riesgo apoyando lo previsto en las normativas ISO 73:2009---ISO/ IEC 31010 :2009 | El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma, los anexos C, D y E hacen referencia la posibilidad de medición del riesgo. | COBIT 5 se alinea con las normas corporativas; COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 3100<br>Con las normas relacionadas a las TI; ISO/IEC 38500, ITIL, serie ISO/IEC 27000, TOGAF (ISACA, 2012) | La norma ISO/IEC 17799 es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado. | ITIL no es medible y puede ser implantado de muchas maneras, mientras que en la ISO/IEC 20000 se evalúa frente a un conjunto establecido de requisitos. |
| CONTEXTO ORGANIZACIONAL | La organización tendrá que determinar el contexto externo e interno que afecta a la organización. | Analiza los aspectos más relevantes que influyen externa e internamente al desenvolvimiento de la organización. | Monitorea y revisa con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana, para mantener una visión general de la perspectiva del riesgo. | Une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores. | Define un conjunto muy amplio de controles de seguridad. No ofrece una solución global al problema de la seguridad porque carece de mecanismos de gestión. | La organización alineara los servicios de las TIC con las necesidades de la empresa o negocio actuales y futuras. |
| SOPORTE | Hace hincapié en la consideración de las capacidades y limitaciones de la organización, así como los recursos que se obtienen de los proveedores externos para la consideración de riesgos | No sólo se refiere a riesgos TIC, sino que se contemplan todo tipo de riesgos. | Aplica la metodología Planificar, hacer, verificar y actuar (PHVA) Al igual que ayuda luego de la valoración del riesgo a la implementación de un plan de tratamiento. | *Satisface las necesidades de las partes Interesadas. *Cubre la Compañía de Forma Integral. *Aplica un solo Marco Integrado. *Habilita un Enfoque Holistico. *Separa el Gobierno de la Administración. | Facilita los requisitos que se deben adoptar, permitirá contar con un manejo adecuado y seguro de la información de la organización ante cualquier posible amenaza. | *Proporciona una clasificacion de roles. *Provee de procesos con indicadores relevantes y mensurables. |
| OPERACIONES | Ambiente de control.<br>*Evaluación de Riesgos.<br>*Actividades de control.<br>*Información y comunicación.<br>*Supervisión. | *Compromiso de dirección.<br>*Diseño del marco de trabajo.<br>* Definición de responsabilidades.<br>*Integración de procesos y mecanismos de comunicación.<br>*Establecer políticas para la Gestión de riesgo. | Establecimiento de plan de comunicación interno y externo.<br>*Definición del contexto organizacional interno y externo.<br>*Valoración de riesgos tecnológicos.<br>*Tratamiento de riesgos tecnológicos. | Evaluación de necesidades de las partes interesadas. *Fijación de directivas para establecimiento de prioridades y toma de decisiones. *Monitoreo del desempeño, cumplimiento y progreso. | Establecer políticas de seguridad.<br>*Organizar la seguridad.<br>*Clasificación y control de activos.<br>*Política de personal.<br>*Seguridad física.<br>*Comunicación y operación.<br>*Control de acceso. | *Administración de configuración.<br>*Administración de incidentes.<br>*Administración de problemas.<br>*Administración de implementación.<br>*Administración de disponibilidad. |
| MEJORAS PARA LA ORGANIZACIÓN | Mejorar la calidad sin malgastar recursos<br>Cumplir con las exigencias legales y reglamentarias, además de las normas internacionales. | Fomentar una gestión proactiva libre de riesgo.<br>Mejorar la identificación de oportunidades y amenazas.<br>Mejorar el aprendizaje organizacional.<br>Mejorar la eficiencia y eficacia operacional. | Aumentar la seguridad y confianza y mejorar la prevención de pérdidas y manejo de incidentes relacionados al manejo de la información.<br>Aplicación satisfactoria de la seguridad de la información. | Construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información. | Recomendaciones de prácticas de seguridad de la información para aquellos interesados en iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. | Mejora la comunicación con los clientes y con los usuarios finales a través de diversos puntos de contacto acordados. |

## Anexo 2 Análisis PHVA

<table>
<tr><th>MODELO PHVA</th><th colspan="3">ISO 27005</th><th colspan="2">ISO 31000</th><th>ISO 9001</th></tr>
<tr><td rowspan="15">PLANEAR</td><td colspan="3"></td><td colspan="2"></td><td>Comprender su organización y su contexto único</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2">Diseño del marco de trabajo para gestión del riesgo</td><td></td></tr>
<tr><td colspan="2" rowspan="5"></td><td rowspan="14">Procesos Gestión del riesgo</td><td colspan="2">Entender la organización y su contexto</td><td rowspan="5"></td></tr>
<tr><td colspan="2">Definir resposabilidades</td></tr>
<tr><td colspan="2">Recursos</td></tr>
<tr><td colspan="2">Integración de procesos</td></tr>
<tr><td colspan="2">Establecer mecanismos de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración del riesgo</td><td rowspan="9"></td><td rowspan="4"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td><td></td></tr>
<tr><td colspan="2"></td><td>Definir acciones para gestionar los riesgos y abordar las oportunidades</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td><td></td></tr>
<tr><td colspan="2"></td><td>Planifique cómo va a gestionar los riesgos y las oportunidades</td></tr>
<tr><td rowspan="3">HACER</td><td colspan="2"></td><td colspan="2">Establecer políticas para la gestión del riesgo</td><td></td></tr>
<tr><td>Implementar el plan de tratamiento</td><td rowspan="2">Implementación del marco de trabajo para la gestión de riesgos</td><td rowspan="2">Implementar el proceso de gestión de riesgos</td><td rowspan="2">Cambio del diseño y desarrollo</td></tr>
<tr><td>Implementar plan de comunicación</td></tr>
<tr><td>VERIFICAR</td><td colspan="2">Monitoreo y revisión del riesgo de TIC</td><td colspan="2">Monitoreo y revisión del marco de trabajo</td><td>Monitorear, medir, analizar, evaluar rendimiento de eficacia</td></tr>
<tr><td>ACTUAR</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td><td>Oportunidades de mejora y acción correctiva</td></tr>
</table>

## Anexo 3 Porcentaje de cumplimiento

| CALIFICACIÓN | GRADO DE CUMPLIMIENTO |
|---|---|
| 0 | No Cunple |
| 1 | Cumple en un nivel muy bajo |
| 2 | Cumple en un nivel medio |
| 3 | Cumple satisfactariamente |
| 4 | Cumple en alto grado |
| 5 | Cumple plenamente |

## Anexo 4 Detalle del calificativo de madurez

| RANGO | NIVEL DE MADUREZ | DESCRIPCIÓN | % CUMPLIMIENTO |
|---|---|---|---|
| 0 - 1.9 | INICIAL | Los procesos relacionados son impredecibles, pobremente controlados y necesitan de mayor atención. | 20% |
| 2 - 2.9 | MANEJADO | Los procesos con el componente evaluado son vistos como actividades a menudos de volver a fallar. | 40% |
| 3 - 3.9 | DEFINIDO | Los procesos son característicos de la organización y son acciones proactivas en algunos o muchos de los casos. | 60% |
| 4 - 4.9 | ADMINISTRADO | Los procesos evaluados son medidos y controlados. | 80% |
| 5 | OPTIMIZADO | Los procesos son enfocados en la mejora continua por ende se esta utilizando una excelente gestión de riesgo de seguridad de información. | 100% |

# Anexo 5 Cumplimiento de normas

| 1. IDENTIFICACIÓN - PLANEAR | | | |
|---|---|---|---|
| CLÁUSULA | VALORACIÓN | NIVEL DE MADUREZ | % CUMPLIMIENTO |
| 4.1 Conocimiento de la Organización y su contexto (ISO 9001) | 3,7 | DEFINIDO | 74% |
| 4.3.1 Entender a la organización y su contexto (ISO 31000) | 3,3 | DEFINIDO | 65% |
| 4.3.3 Rendición de Cuentas (ISO 31000) | 2,8 | MANEJADO | 56% |
| 4.3.4 Integración en los procesos de la organización (ISO 31000) | 2,5 | MANEJADO | 50% |
| 4.3.5 Recursos (ISO 31000) | 2,6 | MANEJADO | 52% |
| 4.3.6 Establecer mecanismos para la comunicación interna (ISO 31000) | 3,0 | DEFINIDO | 60% |
| 4.3.7 Establecer mecanismos para la comunicación externa (ISO 31000) | 4,0 | ADMINISTRADO | 80% |
| 8.2.1 Identificación del Riesgo (ISO 27005) | 2,3 | MANEJADO | 45% |
| 8.2.2.1 Estimación del Riesgo (ISO 27005) | 2,0 | MANEJADO | 40% |
| 8.3 Evaluación del Riesgo (ISO 27005 | 2,0 | MANEJADO | 40% |
| 9. Tratamiento de riesgo | 2,0 | MANEJADO | 40% |
| 6.1 Acciones para tratar riesgo y oportunidades (ISO 9001) | 3,0 | DEFINIDO | 60% |
| 10. Aceptación del Riesgo | 3,0 | DEFINIDO | 60% |
| 6.1.2 La organización debe planificar (ISO 9001) | 3,0 | DEFINIDO | 60% |
| **NIVEL DE MADUREZ DE LA CLÁUSULA** | **2,8** | **MANEJADO** | **56%** |

| 2. APLICACIÓN - HACER | | | |
|---|---|---|---|
| CLÁUSULA | VALORACIÓN | NIVEL DE MADUREZ | % CUMPLIMIENTO |
| 4.3.2 Establecimiento de políticas (ISO 31000) | 3,0 | DEFINIDO | 60% |
| 9.1 Implementación del plan de tratamiento (ISO 27005) | 3,0 | DEFINIDO | 60% |
| 5.2 Comunicación de los riesgos (ISO 27005) | 3,0 | DEFINIDO | 60% |
| 4.4.1 Implementar Marco de referencia (ISO 31000) | 3,0 | DEFINIDO | 60% |
| 4.4.2 Implementar Proceso para la gestión de riesgo (ISO 31000) | 3,0 | DEFINIDO | 60% |
| 8.3.6 Cambio del diseño y desarrollo (ISO 9001) | 3,0 | DEFINIDO | 60% |
| **NIVEL DE MADUREZ DE LA CLÁUSULA** | **3,0** | **DEFINIDO** | **60%** |

| 3. CONTROL - VERIFICAR | | | |
|---|---|---|---|
| CLÁUSULA | VALORACIÓN | NIVEL DE MADUREZ | % CUMPLIMIENTO |
| 12.1 Monitoreo y revisión de los factores de riesgo ( ISO 27005) | 1,8 | INICIAL | 36% |
| 4.5 Monitorear y revisar el marco de referencia (ISO 31000) | 2,5 | MANEJADO | 50% |
| 9.1 Seguimiento, medición, análisis y evaluación (ISO 9001) | 4,0 | ADMINISTRADO | 80% |
| **NIVEL DE MADUREZ DE LA CLÁUSULA** | **2,8** | **MANEJADO** | **55%** |

| 4. MEJORAR-ACTUAR | | | |
|---|---|---|---|
| CLÁUSULA | VALORACIÓN | NIVEL DE MADUREZ | % CUMPLIMIENTO |
| 12.2 Monitoreo, revisión y mejora para la gestión de riesgo (ISO 27005) | 3,5 | DEFINIDO | 70% |
| 4.6 Mejora continua del marco de trabajo (ISO 31000) | 3,0 | DEFINIDO | 60% |
| 10.3 Mejora Continua (ISO 9001) | 3,0 | DEFINIDO | 60% |
| **NIVEL DE MADUREZ DE LA CLÁUSULA** | **3,2** | **DEFINIDO** | **63%** |