# Aspectos de Análisis Gestión de Riesgos, Seguridad y Protección de la Información en las Organizaciones en Colombia

Cruz Garzón, Juan José.
Universidad Piloto de Colombia
Bogotá, D.C.
ingjuancruzg@yahoo.es

*Abstract*— The main purpose of the following paper is to provide the necessary guidelines to understand which are the aspects and the considerations that should be taken when security and information protection are launched, also about how a management risk analysis is generated when it becomes an obligatory topic for most organizations in the country. Nowadays Risk and Administration management is formed as a fundamental part of Organization Management; it pretends to give an efficient support to identification, analysis, treatment, communication and monitoring of business risk when we speak about Information security management system (ISMS).

*Index Terms*—Article 366 of the Constitution, Decree 1537 of 2001, Decree 1599 of May 20/2005, ISO 27001 Management System of the Security Information- ISMS, Government and modeling of information security in organizations Law 489 of 1998, MECI 1000/2005.

*Resumen*—El presente artículo tiene como fin dar las pautas necesarias para entender cuáles son los aspectos y consideraciones que se deben tener en cuenta, a la hora de implementar la seguridad, protección de la información y de cómo se realiza un análisis de gestión de riesgos en el que se convierte en tema de obligatorio para la gran mayoría de Organizaciones del país. Actualmente la Gestión u Administración de Riesgos se constituye como parte fundamental de la Gerencia de la Organización, que pretende respaldar eficientemente a la identificación, análisis, tratamiento, comunicación y monitoreo de los riesgos del negocio cuando se habla de un Sistema de Gestión de la Seguridad de la Información (SGSI) [1].

*Índice de Términos*—Articulo 366 de la Constitución, Decreto 1537 de 2001, Decreto 1599 del 20 de Mayo/2005, ISO 27001 del Sistema de Gestión de la Seguridad de la Información SGSI, Gobierno y modelado de la seguridad de la información en las organizaciones, MECI 1000/2005, Ley 489 de 1998, MECI 1000/2005.

Este artículo se realizó con base a otras fuentes obtenidas desde internet y el formato para la presentación del mismo es IEEE, obtenido desde el link ACIS.

## I. INTRODUCCIÓN

Para la realización de este documento se ha tenido en cuenta factores que enfatizan un entorno de seguridad para brindar la protección a la información., esta se ha convertido en uno de los activos más importantes que toda empresa u organización debe considerar y realizar, teniendo en cuenta sus principales propiedades como son: *Integridad*, *Confidencialidad*, *Disponibilidad*. Para entender y profundizar este tema se ha planteado el siguiente interrogante ¿Qué aspectos y consideraciones se debe tener en cuenta para implementar la seguridad, protección de la información y un buen análisis de gestión de riesgos? Se debe mirar los antecedentes de normas y leyes que permiten dar claridad sobre el proceso y manejo de gestión de riesgos en la *Organizaciones* del país, así mismo para la seguridad y protección de la Información se ha tomado como base de referencia un artículo que habla de estos 2 aspectos importantes, según el artículo "*The Economics of Information Security*", Estoy parcialmente de acuerdo con la opinión de los actores, ya que hay que mirar los temas como de seguridad y protección de la información, lineamientos con la aplicación de la normativa de leyes y diseño general de sistemas --peer to peer, que involucren todos los dueños de los procesos no solo con el área de TICs sino con todas las áreas de la organización, dando como resultado la protección y salvaguardado del activo de la información.

Años atrás estuvo regido por la Norma Australiana AS/NZS 4360. Si hablamos específicamente en Colombia dicha norma fue adaptada bajo el nombre de NTC 5254 en el año

2006 la cual se convirtió en texto obligado al momento de hacer evaluaciones de riesgos para las diferentes organizaciones en Colombia [2]. ¿Qué trata la norma? Básicamente orienta al lector en la necesidad de identificar riesgos que impacten su Organización, Como analizarlos midiendo consecuencia y probabilidad, Evaluar el impacto que tiene la materialización de cada uno de los riesgos identificados, Identificar opciones de manejo de los riesgos (Plan de tratamiento de riesgos); y por último la Medición y análisis de los riesgos. Actualización 2013: La norma actual de gestión de riesgos es la ISO 31000, estándar que realiza un manejo idéntico de la gestión de riesgos al presentado en esta entrada, un ejemplo para control interno de la entidades públicas, se puede ver en la guía de administración de riesgo, en la cartilla de administración pública (Departamento Administrativo de la Función Pública y la Escuela Superior de Administración Publica) [3].

## II. ANÁLISIS GESTIÓN DE RIESGOS

Quiero hacer énfasis a este tema partiendo desde la siguiente premisa: "La medición es el primer paso para el control y la mejora Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se puede controlar, no se puede controlar". [4]

### *A. Identificación de riesgos*

Es importante hacer un levantamiento e identificación de riesgos, para tener una buena administración de los mismos. Para así evitar la posibilidad de ocurrencia de riesgos potenciales, lo cual pueda entorpecer el normal desempeño y desarrollo de las funciones de la organización, para llevar a cabo esta labor se debe elaborar un listado de los riesgos inseparables a las actividades y/o procedimientos que se llevan a cabo en cada uno de los procesos, clasificándolos o priorizándolos según el grado en que estos afecten directamente a los objetivos misionales y metas de la organización.

### *B. Análisis de factores de riesgo*

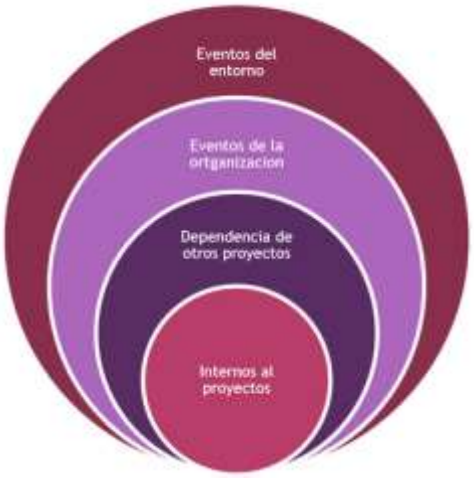
Un buen análisis de factores de riesgos permite tener en cuenta aquellos que pueden incrementar la probabilidad de que un riesgo ocurra. Si no se hace adecuadamente, es posible que se llegue a generar nuevos riesgos como por ejemplo, afectar la integridad, la ética de las personas involucradas, el tamaño y complejidad de las transacciones involucradas en el proceso, finalmente no hay que olvidar que se debe tener en cuenta los factores de carácter externo que pudieran llegar a afectar la organización como son los aspectos económicos, aspectos legales, aspectos sociales o de cambio tecnológico.

### *C. Clasificación del riesgo*

Una vez identificados estos riesgos se debe elaborar una clasificación que permite realizar una mejor identificación de los riesgos inseparables a los procesos de la organización, esta clasificación debe tener unos niveles donde pueda clasificar el riesgo en un nivel de grado que puede ser Alto, Medio y Bajo ya que delimita los parámetros a seguir por el responsable, estos riesgos pueden ser: Estratégicos, Operativo, de Control, Financiero, de Tecnología, de Incumplimiento, de Fraude, de Ambiente Laboral.

A continuación se muestra una imagen que permite visualizar los "Anillos de Riesgos", a los cuales se expone una Organización:

**Fig. 1. Anillos de riesgos, en los cuales se expone una organización [5]**




### *D. Ponderación del riesgo*

Realizada la clasificación de los riesgos, el paso a tener en cuenta es de darles una ponderación a los riesgos que se han detectado, para ello, consiste en establecer los niveles adecuados de calificación, tanto como la probabilidad y el impacto que genera,

esto ayuda a determinar realmente el nivel de vulnerabilidad en que la organización este ante situaciones previsibles. Finalmente se debe tener en cuenta los factores de riesgo enunciados durante el proceso de identificación.

Probabilidad de ocurrencia: este factor se debe considerar los controles utilizados hasta el momento y la efectividad de los mismos, así como, la frecuencia en la que ocurren los riesgos y en la que se van a analizar.

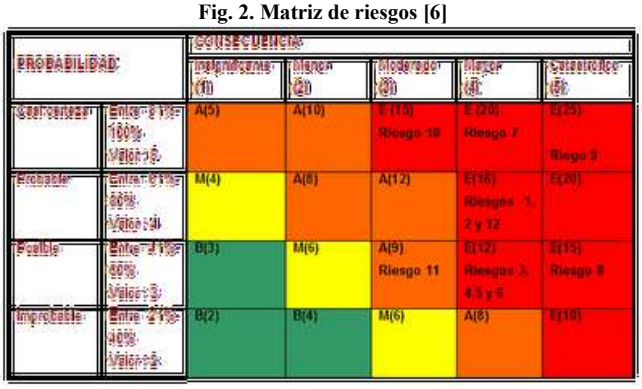
Impacto: en este factor se evalúan las consecuencias en caso que el hecho que originó el riesgo se materialice. También analiza el grado en que afecta los objetivos de los procesos involucrados o, inclusive de manera general a la Organización.

### *E. Manejo del riesgo*

Una vez realizada la Ponderación de los Riesgos, se debe tratar y elaborar un plan de manejo de los mismos. Este plan se debe tener en cuenta la relación costo/beneficio del riesgo que se desea tratar, así como, las consecuencias y las posibles acciones que se van a implementar. La organización puede implementar en este plan una matriz de riesgos donde pueden tener claro que existen varias posibilidades en cuanto a manejo del riesgo. Estas gamas de posibilidades se puntualizan a continuación: 1. Evitar el riesgo, 2. Reducir el riesgo, 3. Trasferir el riesgo, 4. Compartir o diversificar el riesgo, 5. Retener, asumir o aceptar el riesgo. En el siguiente control permite dar un mayor entendimiento más clara de lo que se debe hacer para el manejo de los riesgos, a través de una matriz de ejemplo.

### *F. Descripción de la matriz de riesgos*

**Fig. 2. Matriz de riesgos [6]**




Los conceptos para la información en el que se debe manejar para la administración del riesgo, se debe referir a lo siguiente:

- Riesgo: este concepto define la posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la Organización y le impidan el logro de sus objetivos.
- Impacto: para muchos gerentes es importante este concepto ya que define cuales son las consecuencias que puede ocasionar a la organización la materialización del riesgo
- Probabilidad: este concepto determina la posibilidad de ocurrencia y/o frecuencia del riesgo detectado.
- Control existente: en este concepto se debe especificar cual es el control que la Entidad u organización tiene implementado para combatir, minimizar o prevenir el riesgo.
- Nivel de Riesgo: es el concepto donde ofrece el resultado de la aplicación de la escala escogida para determinar el nivel de riesgo de acuerdo a la posibilidad de ocurrencia, teniendo en cuenta los controles existentes.
- Causas: este concepto es también importante ya que son todos los medios, circunstancias y agentes que generan los riesgos.
- Acciones: el concepto define que se debe tener en cuenta la aplicación concreta de las opciones del manejo del riesgo, acciones correctivas y/o preventivas, que entraran a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.
- Responsables: es muy importante este concepto, ya que la mayor debilidad para implementar la seguridad de la Información son las personas, un mal entrenamiento y conciencia de cultura en toda la organización es un factor importante a tener en cuenta, las dependencias o áreas encargadas de adelantar las acciones propuestas, también se deben determinar en cabeza de quien va a quedar el compromiso del cumplimiento, de las entregas, monitoreo (auditorias) y mejoras para el sistema de seguridad de la Información.
- Cronograma: Estos comprende un herramienta eficiente son las fechas establecidas para

implementar las acciones por parte del grupo de trabajo.

- Indicadores: es otro concepto importante, indica realmente como esta o en que avance esta la organización, se emplea para evaluar el desarrollo de las acciones implementadas y pueden ser de tipo cuantitativo o cualitativo, es el resultado de la evaluación donde permite emitir un juicio mediante su utilización y cumplir así el uso de la metodología dentro de un proceso de mejora continua.

### *G. Plan de manejo del riesgo*

Teniendo claro los posibles manejos que se le da a cada riesgo y que se han mencionado anteriormente, se deben formular acciones para su realización, estableciendo responsables de estas y fijando fechas para su desarrollo. Los responsables también deben velar por el cumplimiento en el desarrollo e implementación de los puntos de control. Tal como se mencionó previamente se encuentran las diferentes alternativas del manejo del riesgo, las cuales serán tenidas en cuenta para el Monitoreo de los Riesgos recordemos, nuevamente se destacan estos criterios, que según la organización debe considerar: Evitar el riesgo, Reducir el riesgo, Transferir el riesgo, Compartir o diversificar el riesgo, Retener, asumir o aceptar el riesgo.

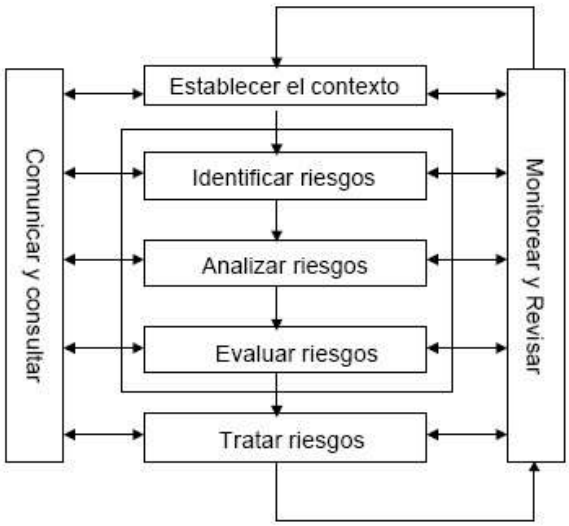
### *H. Ejecución del plan de manejo de riesgos*

Básicamente esta ejecución del plan de manejo de riesgos radica y enfatiza a la realización de un monitoreo de las matrices de riesgos de las diferentes áreas en la organización, estas se deben presentar en reuniones periódicas; en donde cada uno de los responsables de los procesos de la organización estará encargado de complementar y actualizar sus matrices a medida que surgen nuevos riesgos o si los controles aplicados logran reducir o incluso eliminar los riesgos existentes.

Pasos a seguir por proceso para realización del monitoreo [7]:

- Revisar cuidadosamente la última matiz de riesgos aprobada.
- Listar las medidas existentes o planeadas para reducir la ponderación del riesgo. Se listaran medidas para reducir la probabilidad y para reducir el impacto.
- Evaluar si los riesgos y las causas que los originaron persisten, de ser así confirme que los controles de estos riesgos no se hayan modificado o tergiversado con el tiempo.
- Proponer nuevos controles para los que son obsoletos.
- Considerar el (los) riesgo(s) que han desaparecido y con base en esto elaborar un informe explicando su apreciación para que éste sea retirado del mapa oficial del área.

**Fig. 3. Ciclo del análisis de riesgos [8]**




### *I. Metodologías utilizadas para la gestión de riesgos*

A continuación se referencia las metodologías más conocidas de análisis y gestión de riesgo: Herramienta OCTAVE, Herramienta MAGERIT, Herramienta EAR/PILAR, Herramienta CRAMM, ISO 27000 e ISO 31000. Estas se pueden elegir según el criterio aprobado por la organización, es de entender el nivel complejidad que tenga cada una de estas y que realmente se escoja la que más criterio se ajuste a los procesos que actualmente tiene la organización o entidad.

Una vez identificado estos aspectos de riesgos y vulnerabilidades en nuestra organización, se puede decir en cierta manera, que se está brindado seguridad y protección a nuestra información que corresponde a un ciclo maduro y mejora continua.

## III. SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Desde mi punto de vista con lo que he investigado en fuentes de internet, he escogido un artículo interesante "*The Economics of Information"* [9] El cual hago un aporte que consiste --Determinar el entorno de seguridad de la información como un todo independiente a cada una de las organizaciones, ya que la seguridad enfatiza desde lo físico en general, la integración con los procesos que cuenta cada una de las organización, el grado de protección de los activos que deseamos proteger, la tecnología que se requiera implementar, los mecanismos y controles de procedimientos, políticas, la medición de los riesgos que podamos mitigar, la relación de los Beneficios/costos que designemos para ello, proporcionando y generando así, el sistema de la gestión de la seguridad de la información.

Es por ello que este sistema de gestión de la seguridad de la información debe que hacerse cuidadosamente, para garantizar aspectos principales como: confidencialidad, integridad y Disponibilidad, posteriormente una vez que tengamos claro estos 3 conceptos, se procede a definir nuestro sistema de gestión, el cual nos sirve como principios de diseño para la implementación de la seguridad., estos principios lo definen los autores (SALTER y SCHODER) de la siguiente manera: --el diseño debe ser público, --el estado por defecto debe ser el de <No Acceso>, --la verificación debe ser activa y continua, dar a la entidades el mínimo privilegio posible, --el mecanismo de protección debe ser simple, uniforme e integrado (no es un valor añadido, sino una característica a todos los niveles), --debe ser psicológicamente aceptable por los usuarios [10].

Una vez entendido lo anteriormente, se debe tener y definir una metodología para la realización y sostenimiento continuo de nuestro sistema de gestión de la seguridad, La norma ISO/27001 brinda esta pauta., el Dr. Carlos Manuel Fernández, Coordinador de TIC de AENOR, en su artículo sobre esta norma exalta que es la solución de mejora continua más adecuada para evaluar los riesgos físicos y lógicos, así como establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información [11].

Finalmente, podemos ver un ejemplo de un estudio sobre el entorno de Gobierno centrado en la norma ISO/27001 aplicando diferentes de modelos de procesos, bajo normativa legal vigente de un buen gobierno y modelado de la seguridad de la información en las organizaciones. Realizado por la autora Sandra Ontoria Gonzalo de la Escuela Politécnica de Madrid. Ver link en la referencia bibliográfica citada [12].

## IV. CONCLUSIONES

1. Se tiene diferentes Metodologías para la implementación de gestión de riesgos en las Organizaciones, cada una de estas es libre en elegir la de su preferencia o la más apropiada para aplicarla a su gobierno, siempre y cuando se tenga claro, que es lo que se quiere hacer y el buen conocimiento de la metodología para su implementación.
2. La decisión final sobre la evaluación de Riesgos la toma la Alta Gerencia, previo antes de ser considerada por los dueños de los diferentes procesos, esto se debe realizar y presentar periódicamente en las reuniones realizadas con los altos directivos, el nivel de tolerancia de este resultado debe estar en un nivel aceptable para las organizaciones.
3. La gestión de riesgos es la única forma de poder medir y aminorar la inseguridad ya que esta es una propiedad inherente a los recursos informáticos.
4. En Colombia las normas de mayor auge para la gestión de los riesgos en las organizaciones son la ISO 27001:2005 (su nueva versión es la ISO 27001:2013) sobre Sistemas de Gestión de Seguridad de la Información – SGSI y la ISO 31000 sobre Gestión del Riesgo, Principios y Directrices.
5. Para garantizar un sistema de gestión de la seguridad de la información, debe tener en cuenta los aspectos de principales de Confidencialidad, Integridad y Disponibilidad.

## REFERENCIAS


[1] Gestión de riesgos. Página web, Seguridad de la información en Colombia. Mayo, 2010. Web de referencia: http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[2] Norma Técnica Colombiana NTC 5254: Gestión del Riesgo. Editada por Instituto Colombiano de Normas Técnicas y Certificación INCONTEC. 2004. Bogotá.

[3] Cartillas sobre Administración Publica: Guía de Administración del Riesgo. DAFP – ESAP. Cuarta Edición. Noviembre de 2009. Bogotá. Web de referencia: http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=558

[4] Documento: El Análisis Riesgos Base Sistema Gestión Seguridad Información Caso Magerit.pdf, Web de referencia: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

[5] Anillos de riesgos, en los cuales se expone una organización. Página web, Seguridad de la información en Colombia, gestión de riesgos. Mayo, 2010. Web de referencia: http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html.

[6] Matriz de riesgos. Página web, Seguridad de la información en Colombia, gestión de riesgos. Mayo, 2010. Web de referencia: http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[7] Pasos a seguir por proceso para realización del monitoreo. Página web, Seguridad de la información en Colombia, gestión de riesgos. Mayo, 2010. Web de referencia: http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[8] Ciclo del Análisis de Riesgos. Página web, Seguridad de la información en Colombia, gestión de riesgos. Mayo, 2010. Web de referencia: http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[9] Aspectos económicos de la seguridad. Artículo «The Economics of Information Security». Web de referencia: http://lyle.smu.edu/~tylerm/science-econ.pdf

[10] DITEC. (2009). SEGURIDAD Y PROTECCIÓN. 2009, de Sistemas Operativos. Sitio Web de referencia: http://www.ditec.um.es/so/apuntes/teoria/tema7.pdf

[11] CARLOS MANUEL FERNANDEZ. (2012). La norma ISO 27001 del sistemas de gestión de la información. 2012, de Seguridad. Web de referencia: http://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

[12] SANDRA ONTORIA GONZALO - ESCUELA POLITÉCNICA DE MADRID. (2011). Gobierno y modelado de la seguridad de la información en las organizaciones. 2014, de Ingeniería Técnica en Informática de Gestión. Web de referencia: http://orff.uc3m.es/bitstream/handle/10016/11898/PFC_Sandra_Ontoria_Gonzalo_Final.pdf?sequence=1


**Autores**


Realizado por:
JUAN JOSÉ CRUZ GARZÓN. Ingeniero de Sistemas - Universidad Cooperativa de Colombia, certificación en CCNA – U. Tolima, diplomado en Auditoria de Sistemas y Telecomunicaciones - ITFIP, diplomado en Liderazgo – E.S.A.P Y C.A.F. experiencia como Ingeniero de soporte en Bases de Datos – I.C.B.F, Docente de Tecnologia Colegio Fidel Cano, Especialista Junior Siebel – S.Q.D.M, Actualmente soy el Administrador de Redes del Instituto Nacional de Cancerología.
Estudiante de Postgrados
Especialización en Seguridad Informática
Universidad Piloto de Colombia
2014


*"Este documento está diseñado para profundizar el conocimiento del área de Gestión de la Informática y es de carácter Académico".*