ESTUDIO ANALÍTICO DE LA COMPATIBILIDAD E INTEGRACIÓN DE LAS NORMAS ISO/IEC 31000 E ISO/IEC 27005 REFERENTE A RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

Myrian Alexandra Medina Tapia
Escuela Politécnica del Ejército,
miriam.medina.tapia@gmail.com

RESUMEN

Mediante la utilización de mapeos de alto nivel y mapeos detallados de estructuras, procesos, conceptos y anexos, se confirmó la factibilidad acerca de la integración de los estándares ISO/IEC 31000 e ISO/IEC 27005. En el trabajo se determinó que la diferencia básica entre las normas es que ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que ISO/IEC 27005 lo hace de forma específica en la Gestión de los Riesgos en la Seguridad de la información. La norma ISO/IEC 27005 identifica de forma minuciosa los activos, los impactos y las amenazas a las que estos activos están expuestos, a más de realizar el análisis de las vulnerabilidades y de los riesgos a nivel alto y detallado. Sin embargo los fundamentos organizacionales, la forma de planificar y ejecutar los proyectos y procesos son similares en ambas normas.

Como resultado final el trabajo se obtuvo un documento útil para aplicarlo en el proceso de gestión de riesgos de seguridad de la información, sobre la base de la integración de las dos normas involucradas.

***Palabras Clave**:* Seguridad de la Información, Gestión de Riesgos, ISO/IEC 31000, ISO/IEC 27005, Integración de estándares

ABSTRACT

This paper attempts to describe risk assessment methodologies for IT Security, ISO/IEC 3100 and ISO/IEC 27005 standards; perform compatibility analysis between the two norms and an integration model. From the investigation done using high-level mapping and detailed structures, processes, concepts and annexes, the possibility of integrating these two norms is feasible. The basic difference between the norms is that that ISO / IEC 31000 focus on comprehensive risk management and generic, whereas ISO / IEC 27005 specifically focus in Risk Management in Information Security. ISO / IEC 27005 thoroughly identify assets, impacts and threats to which these assets are exposed, as well as vulnerability breakdown, high and detailed level risks. However organizational fundamentals, how to plan and implement projects and processes are similar in both standards.

As a final result work useful to apply in the risk management process of information security, based on the integration of the two standards involved document was obtained.

Keywords: Information Security, Risk Management, ISO/IEC 31000, ISO/IEC 27005, integration of standards

1. **INTRODUCCIÓN**

De las investigación bibliográfica realizada, hasta el momento no existen estudios en el Ecuador acerca de la complementariedad de las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008) relacionada a gestión de riesgos en la seguridad de la información.

El estudio describe la compatibilidad e integración del estándar ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008) en lo referente a Riesgos en la Seguridad de la Información. La adopción de principios y la implementación de las normas ISO 31000 (ISO, 2009) e ISO 27005 (ISO, 2008) y su aplicación incluyen actividades como estrategias, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

2. CRITERIOS DE COMPARACION E INTEGRACION

A partir de un análisis e las normas ISO/IEC 31000 e ISO/IEC 27005 se determina que los parámetros que deben ser seleccionados para realizar una comparación entre ellas son: la estructura, los procesos básicos, los conceptos y los anexos. A continuación se presentan mapeos de alto nivel de los procesos y un mapeo detallado de los anexos que servirá para ejemplificar la afirmación.

2.1 Mapeo de Procesos de Alto Nivel

Al realizar el análisis de los procesos de la gestión del riesgo de las normas, se determinó que en todos ellos se realizan actividades similares, lo cual se puede visualizar en la tabla que se detalla a continuación:

Tabla 1
ISO 27005 vs Procesos Mapeados de alto nivel de ISO 31000

ISO 31000 Procesos y Dominios	ISO 27005 Establecimiento del Contexto	ISO 27005 Valoración del Riesgo	ISO 27005 Tratamiento del Riesgo	ISO 27005 Comunicación del Riesgo	ISO 27005 Monitoreo y Revisión del Riego
Comunicación y Consulta	“0”	“0”	“0”	"+"	“0”
Establecimiento del Contexto	"+"	"0"	“0”	“0”	“0”
Valoración del Riesgo	0	"+"	“0”	“0”	“0”
Tratamiento del Riesgo	"-"	“0”	"+"	"+"	“0”
Monitoreo y revisión	“0”	“0”	“0”	“0”	"+"
Registro del proceso para la gestión del riesgo	"-"	"-"	"-"	"-"	"-"

(+) Coincidencia significativa (6)
(0) Coincidencia menor (18)
(-) Enfoque menor o no relacionado (6)

El análisis del nivel de coincidencia en los procesos de alto nivel determina que existen, 6 “+”, 18 “0” y 6 “-”, lo que indica que a nivel de procesos existe complementariedad entre las ambas normas, ya que de un total de 30 opciones, 24 demuestran un nivel de coincidencia, y solo 6 presentan un nivel de enfoque menor o no relacionado.

2.2 Mapeo de Anexos

En la tabla 2 se presenta un análisis del contenido de los anexos que utilizan las normas y se determina si existe o no un nivel de coincidencia o complementariedad entre ellos.

Tabla 2
Mapeo de Anexos

Anexo	ISO 31000 Definición	ISO 27005 Definición	Comentarios	Nivel de Coincidencia
Norma ISO/IEC 31000 – Anexo A	*Atributos de la gestión mejorada del riesgo* • Mejora continua • Rendición de cuentas en relación a los riesgos • Aplicar la gestión del riesgo en la toma de decisiones • Comunicaciones continuas con los involucrados • Integración en la estructura organizacional.	n/a	La norma ISO 27005 no incluye un anexo relacionado a atributos para la gestión del riesgo, sin embargo a nivel de procesos los analiza.	"+"
Norma ISO/IEC 27005 - Anexo A	n/a	*Definición del alcance y los límites del proceso de la gestión del riesgo en la seguridad de la información*	La norma ISO 31000 no analiza el riesgo en la seguridad de la información	"-"
Norma ISO / IEC 27005 - Anexo B	n/a	• *Pérdidas basadas en impactos operacionales (directos e indirectos)* • *Comparación de impactos operacionales directos* • *Impactos operacionales indirectos*		"-" "-" "-"
Norma ISO / IEC 27005 Anexo C	n/a	*Ejemplos de Amenazas Comunes: deliberadas, accidentales y ambientales.*	La norma ISO/IEC 31000 no analiza ningún tipo de amenazas.	"-"
Norma ISO / IEC 27005 – Anexo D	n/a	*Vulnerabilidades y Métodos para valoración de vulnerabilidades. (hardware, software, red, personal, lugar y organización)*	La ISO 31000 no menciona la vulnerabilidad de los activos y/o la probabilidad de que este sea incapaz de resistir las acciones de una amenaza.	"-"
Norma ISO/IEC 27005 – Anexo E	n/a	Enfoques para la valoración de riesgos en la seguridad de la Información. (alto nivel y detallada)	La norma ISO/IEC 31000 no hace un análisis sobre los riesgos en la seguridad de la información.	"-"
Norma ISO/IEC 27005 – Anexo F	n/a	Restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, de personal y de integración de controles para la reducción del riesgo.	La norma ISO/IEC 31000 no describe las restricciones relacionadas a la reducción del riesgo.	"-"

(+) Coincidencia Significativa (1)
(0) Coincidencia menor (0)
(-) Enfoque menor o no relacionado (6)

El mapeo de anexos indica, que el Anexo A de la ISO/IEC 31000 (ISO, 2009), tiene una coincidencia significativa a nivel de procesos con la ISO/IEC 27005 (ISO, 2008). Sin embargo los 6 anexos de la ISO/IEC 27005 (ISO, 2008), no tienen ningún tipo de relación con la ISO/IEC 31000 (ISO, 2009), lo cual constituye una de las grandes diferencias entre ambas normas.

3. INTEGRACION DE LAS NORMAS ISO/IEC 31000 E ISO/IEC 27005

Como se ha indicado previamente es factible integrar las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008) entre sí, debido a la complementariedad y aproximación existente, lo que se ve reflejado en el mapeo de alto nivel y específico presentado en el apartado anterior.

Por razones de espacio, a continuación se presentan dos ejemplos de integración.

Ejemplo No. 1: Integración de Procesos

PROCESOS ISO/IEC 31000:

5	PROCESO
5.a	Generalidades
5.b	Comunicación y Consulta
5.c	Establecimiento del contexto
5.d	Valoración del riesgo
5.d1	*Identificación del riesgo*
5.d2	*Análisis del riesgo*
5.d3	*Evaluación del riesgo*
5.e	Tratamiento del riesgo
5.e1	*Selección de opciones*
5.e2	*Preparación e implementación de planes*
5.f	Monitoreo y Revisión
5.g	Registro del Proceso para la gestión del Riesgo

PROCESOS ISO/IEC 27005

6	Visión General del proceso
7	Establecimiento del Contexto
7.1	*Consideraciones Generales*
7.2	*Criterios básicos*
7.3	*El alcance y los límites*
7.4	*Organización para la gestión del riesgo*
8	Evaluación del Riesgo
8.1	*Descripción de la valoración del riesgo*
8.2	*Análisis del riesgo*
8.2.1	*Identificacion del riesgo*
8.2.2	*Estimación del riesgo*
8.3	*Evaluación del riesgo*
9	Tratamiento del riesgo
9.1	*Descripción general*
9.2	*Reducción del riesgo*

9.3	*Retención del riesgo*
9.4	*Evadir el riesgo*
9.5	*Transferencia del riesgo*
10	Aceptación del riesgo en la seguridad de la información
11	Comunicación de los riesgos
12	Monitoreo y Revisión del riesgo en la seguridad de la información
12.1	*Monitoreo y revisión de los factores de riesgo*
12.2	*Monitoreo, revisión y mejora de la gestión del riesgo*

DOCUMENTO INTEGRADOR DE PROCESOS DE LAS NORMAS ISO/IEC 31000 E ISO/IEC 27005

A continuación se describe un documento que integra los procesos las normas que son objeto de este estudio. El marco de la norma integrada será la norma ISO/IEC 31000.

Estructura de la Norma

Esta norma contiene la descripción de los procesos para la gestión del riesgo de la seguridad de la información, basada en las normas ISO/IEC 31000 e ISO/IEC 27005. Las actividades son: la comunicación y consulta, el establecimiento del contexto, la valoración, el tratamiento, la aceptación, y el monitoreo y la revisión del riesgo en la seguridad de la información.

La estructura de cada actividad está compuesta por:

a) ***Entrada***: identificar la información que se requiere para realizar la actividad
b) ***Acciones:*** describe la actividad
c) ***Guía de implementación:*** proporciona guías para ejecutar la acción
d) ***Salida:*** identificar la información generada después de realizar la actividad.

Comunicación y consulta

El proceso de comunicación y la consulta se realiza durante todas las etapas del proceso de gestión del riesgo. Los planes que se elaboren deben considerar la identificación del riesgo, las causas que lo originan, sus consecuencias, y la forma en que el riesgo debe ser tratado. Los involucrados en el proceso de gestión de riesgo deben ser informados de las decisiones adoptadas.

Establecimiento del contexto

Establecer el contexto implica articular los objetivos, definir los parámetros y establecer el ámbito de aplicación, para lo cual crear una estructura que implemente y mantenga el proceso de la gestión del riesgo en la seguridad de la información es indispensable. Además Se debe considerar el alcance, las responsabilidades y las barreras organizacionales existentes y definir los criterios básicos para gestionar, evaluar y aceptar el riesgo.

Valoración del riesgo de la seguridad de la información

La valoración del riesgo incluye las actividades de identificación, análisis y evaluación de riesgos. En esta etapa se elabora una lista de todos los riesgos y se analiza las causas, las fuentes de riesgos, las consecuencias y la probabilidad de ocurrencia. Además se evalúa el proceso de toma de decisiones, a través del uso de criterios de comparación, que permitan determinar cómo tratar el riesgo.

Identificación de Riesgos

Se determina activos, amenazas, controles, procesos de negocios y las vulnerabilidades de los activos ante las amenazas. Se analiza además las consecuencias por pérdida de confidencialidad, integridad y disponibilidad de los activos. El propósito de la identificación del riesgo es determinar qué factores podrían causar una pérdida potencial y cuáles son los motivos.

Análisis y Estimación de Riesgos

Evaluar el riesgo implica definir parámetros de entrada, métodos y estrategias para analizar e identificar las causas que originan los riesgos, y adoptar decisiones que pueden generar riesgos distintos.

Analizar los riesgos, es determinar su probabilidad de ocurrencia y su impacto. Al valorar los riesgos se debe identificar si son integrables entre sí, y si dependen unos de otros. El nivel del riesgo es una variable que indica todo lo que se ha asumido. La probabilidad de ocurrencia, se obtiene a través de modelar los resultados de uno o varios eventos, extrapolando los valores de los datos disponibles. El impacto de un riesgo, si este ocurre, puede ser tangible o intangible y afectar la confidencialidad, integridad y disponibilidad de los activos del negocio.

La información de la que se disponga permitirá realizar un análisis cualitativo o cuantitativo del riesgo, lo cual dependerá a su vez del tipo del riesgo, el objetivo del análisis y los recursos de los que se disponga. Es necesario evaluar las amenazas y las vulnerabilidades producidas por incidentes de seguridad de la información; y determinar el nivel del riesgo ante incidentes relevantes.

Tratamiento del riesgo de la seguridad de la información

Los riesgos pueden modificarse, si al ser evaluados, se requiere adoptar medidas para reducir o eliminar su impacto. Si se detecta que el riesgo residual no es tolerable se debe seleccionar una alternativa distinta y evaluar sus resultados. La probabilidad de que un riesgo se incremente es alta, si se decide, que es indispensable para lograr un objetivo organizacional.

Selección de Opciones

Tratar el riesgo requiere mantener un equilibrio entre los costos de implementación y los beneficios que se esperan obtener, para lo cual conocer que riesgos son graves, de baja probabilidad y de alto costo para la organización es crítico. Las opciones para tratar el riesgo son reducir, retener, evitar y transferir el riesgo.

Preparación e implementación de planes

En esta etapa se documenta las opciones seleccionadas, los beneficios esperados, el proceso de implementación y el cronograma del plan del tratamiento del riesgo, el cual debe incluir los riesgos secundarios.

Monitoreo y Revisión **del** *riesgo de la seguridad de la información*

El monitoreo del riesgo a nivel de seguridad de la información, consiste en valorar el riesgo y el contexto en el que este se desenvuelve. Se evalúa si el proceso es el apropiado y si existen nuevos riesgos o cambios en los existentes, que puedan ocasionar nuevas amenazas, vulnerabilidades o situaciones que se consideren inaceptables. Se realiza una grabación del proceso, para obtener la trazabilidad que permita mejorarlo si se requiere.

Registro del proceso para la gestión del riesgo

Al realizar la trazabilidad del proceso de gestión del riesgo y sus actividades se debe estimar la información sensible a ser almacenada y los costos que implican almacenar, recuperar y dar mantenimiento a la misma.

Los atributos e indicadores que muestran el nivel de desempeño en el proceso de la gestión del riesgo son: la mejora continua, la rendición de cuentas, la aplicación de la gestión del riesgo en la toma de decisiones, las comunicaciones continuas y la integración completa en la estructura de la organización.

El proceso de mejora continua define indicadores que miden la existencia de metas explicitas de desempeño de gestión del riesgo a nivel individual u organizacional. Los resultados de esta evaluación deben ser analizados antes de determinar los objetivos del siguiente año.

La rendición de cuentas consiste en informar a la organización sobre las actividades de control y monitoreo que fueron realizadas para tratar el riesgo. Un equipo de trabajo que incluya a directores, especialistas en sistemas de información y a los de forma exhaustiva. Se requiere un nivel de jerarquía y autoridad necesaria para cumplir con los objetivos planteados.

El proceso de toma de decisiones es medida a través de un indicador que determina que fue analizado y discutido, las decisiones que se adoptaron, y su relación con el riesgo.

El desempeño de la gestión del riesgo y la forma como los riesgos significativos han sido manejados deben ser comunicados a la Organización. Las decisiones adoptadas deben ser acordes al nivel del riesgo asumido y el tratamiento realizado para bajar su impacto.

Integrar el proceso de la gestión del riesgo en la estructura de la organización, es posible mediante el uso de indicadores que permitan determinar si un objetivo será alcanzado.

Ejemplo No. 2 Integración de Anexos

Anexos de la Norma ISO/IEC 31000

Documento Origen	Descripción del Anexo
Anexo A ISO/IEC 31000	Atributos de la gestión mejorada del riesgo • Mejora continua de la gestión del riesgo • Rendición total de cuentas con respecto a los riesgos • Aplicación de la gestión de riesgos en la toma de decisiones de la organización • Comunicaciones continuas

Anexos de la Norma ISO/IEC 27005

Documento Origen	Descripción del Anexo
Anexo A ISO/IEC 27005	Definición del alcance y los límites del proceso de la gestión del riesgo en la seguridad de la información.
Anexo B ISO 27005	Identificación y valoración de los activos y valoración de los impactos • Perdidas basadas en impactos operacionales • Comparación de impactos operacionales directos • Impactos operacionales indirectos
Anexo C - ISO 27005	Ejemplos de Amenazas Comunes: deliberadas, accidentales y ambientales.
Anexo D - ISO 27005	Vulnerabilidades y Métodos para la valoración de vulnerabilidades
Anexo E - ISO 27005	Enfoques para la valoración de riesgos en la seguridad de la Información.
Anexo F - ISO 27005	Restricciones para la reducción del riesgo.

INTEGRACION DE ANEXOS DE LAS NORMAS ISO/IEC 31000 e ISO/IEC 27005

Finalmente, se detalla a continuación la integración de los anexos de las normas ISO/IEC 31000 e ISO/IEC 27005:

Tabla 3
Integración de Anexos

Documento Origen	Descripción del Anexo
Anexo A ISO/IEC 31000	Atributos de la gestión mejorada del riesgo • Mejora continua de la gestión del riesgo • Rendición total de cuentas con respecto a los riesgos • Aplicación de la gestión de riesgos en la toma de decisiones de la organización • Comunicaciones continuas
Anexo A ISO/IEC 27005	Definición del alcance y los límites del proceso de la gestión del riesgo en la seguridad de la información.
Anexo B ISO 27005	Identificación y valoración de los activos y valoración de los impactos • Perdidas basadas en impactos operacionales • Comparación de impactos operacionales directos • Impactos operacionales indirectos
Anexo C - ISO 27005	Ejemplos de Amenazas Comunes: deliberadas, accidentales y ambientales.
Anexo D - ISO 27005	Vulnerabilidades y Métodos para la valoración de vulnerabilidades
Anexo E - ISO 27005	Enfoques para la valoración de riesgos en la seguridad de la Información.
Anexo F - ISO 27005	Restricciones para la reducción del riesgo.

Al unificar los anexos, se puede visualizar que mientras la ISO/IEC 31000 (ISO, 2009) se enfoca en los atributos para realizar una mejora continua y una evaluación del proceso de gestión de riesgos a nivel de toda la organización, la ISO/IEC 27005 (ISO, 2008), en cambio baja de nivel y define el alcance del proceso, y especifica las actividades. Identifica y valora de forma minuciosa los activos, las amenazas, las vulnerabilidades y las consecuencias. Por último realiza una valoración de alto nivel y detallada de los riesgos en la seguridad de la información y las restricciones que pueden afectar la reducción de los mismos.

4. DISCUSION DE RESULTADOS Y CONCLUSIONES

Como resultado de este estudio se determinó la factibilidad de integración y complementariedad de las normas ISO/IEC 31000 e ISO/IEC 27005, mediante la utilización de mapeos de alto nivel y detallados de las estructuras, procesos, conceptos y anexos.

El análisis de similitudes y diferencias demostró que la norma ISO/IEC 31000 se enfoca en la Gestión de Riesgos de manera integral, mientras que la ISO/IEC 27005 es específica en la Gestión de Riesgos en la Seguridad de la Información.

Al analizar los conceptos utilizados se determina que provienen del mismo origen que son la Guía ISO 73:2009 y las normas ISO/IEC 27001 e ISO/IEC 27002.

A nivel de anexos la diferencia básica encontrada es que la ISO/IEC 31000 se enfoca en los atributos que debe tener la gestión del riesgo, mientras que la ISO/IEC identifica y analiza los riesgos, los activos, impactos, amenazas y vulnerabilidades.

El desarrollo del modelo integrado demuestra la consistencia del análisis realizado basado en las normas objeto del estudio.

5. REFERENCIAS

BSI UK. (2013). Transition Guide - Moving from ISO 27001:2005 to ISO 27001:2013. Milton Keynes, United Kingdom. Obtenido de www.bsigroup.com/27books.

Dali, A. (2009). Les enjeux de la norme ISO 31000 en gestion des risques. *la tribune de l'assurance • n° 133 •février 2009*, 60-61.

Ferma. (2003). *Estándares de Gerencia de Riesgos.* Bruselas: Federation of European Risk Management Associations.

Henning, D. (22 de 07 de 2009). *TACKLING ISO 27001: A project to buid an ISMS.* Obtenido de ISO WEB SITE: http://www.iso27001security.com/GIAC_GCPM_gold_henning.pdf

ISO. (2005). *27001 Information technology - Security techniques - Information Security Management Systems - Requirements.* Ginebra: International Organization for Standarization y International Electrotechnical Comission.

ISO. (2005). *ISO/IEC 27002 Information Tecnhology - Security Techniques - Code of practiece for Information Security Management.* Ginebra: International Organization for Standarization y International Electrotechnical Comission.

ISO. (2008). *27005:2008 Information Technology - Security Techniques - Information Security Risk Manegement.* Ginebra: International Organization for Standarization y International Electrotechnical Comission.

ISO. (2009). *ISO Guide 73:2009 Risk manegement - vocabulary.* Ginebra: International Organization for Standarization.

ISO. (2009). *ISO/IEC 31000:2009, Risk Management - Principles and guidelines.* Ginebra: Internacional Organization for Standarization y International Electrotechnical Comission.

ISO. (2009). *ISO/IEC 31010:2009 Técnicas de evaluación de Riesgos e interpretación de la norma ISO 31000:2009.* Ginebra: International Organization for Standarization y International Electrotechnical Comission.

ISO. (2011). *ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.* Ginebra: International Organization for Standarization y International Electrotechnical Comission.

IT GOVERNANCE. (October de 2013). *it Governance Comparing ISO 27001:2005 to ISO 27001:2013.* Obtenido de IT GOVERNANCE Web site: www.itgovernance.co.uk

IT GOVERNANCE INSTITUTE. (2008). *Alineando COBIT 4.1 ITIL V3 Y ISO/IEC 27002 en beneficio de la empresa.* Obtenido de ISACA WEB SITE: www.isaca.org/cobit

IT GOVERNANCE INSTITUTE. (2008). *COBIT MAPPING - Mapping of ITIL v3 With COBIT4.1.* Obtenido de ITGI WEB SITE: www.itgi.org

Merkelbach, Martin; Daudin, Pascal. (2011). *From Security Management to Risk Management.* Obtenido de Security Management Initiative Web site: www.security-- management-- initiative.org

THE OPEN GROUP. (October de 2010). *Technical Guide FAIR-ISO/IEC 27005 Cookbook.* Obtenido de THE OPEN GROUP: www.opengroup.org

Tres PASS Project. (31 de 10 de 2014). *Currently established risk-assessment.* Obtenido de Tres PASS Web site: http://www.trespass-project.eu/