DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA INGENIERÍA EN SISTEMAS E INFORMÁTICA

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

"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"

AUTOR: MYRIAN ALEXANDRA MEDINA TAPIA

DIRECTOR: ING. CARLOS MONTENEGRO

SANGOLQUÍ, JULIO 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICADO

Yo, Carlos Montenegro, en calidad de Director de Tesis, certifico que el trabajo titulado “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”, realizado en su totalidad por la Srta. Myrian Alexandra Medina Tapia ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la Universidad de las Fuerzas Armadas – ESPE.

El mencionado trabajo consta de un documento empastado y un disco compacto, el cual contiene los archivos en formato portátil de Acrobat (PDF). Se autoriza a la Srta. Myrian Alexandra Medina Tapia, la entrega del material Ing. Mauricio Campaña, Director de la Carrera de Ingeniería de Sistemas e Informática.

Sangolquí, Julio del 2015

Ing. Carlos Montenegro
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICADO

Yo, Carlos Montenegro, en calidad de Director de Tesis, certifico que el trabajo titulado “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”, fue realizado en su totalidad por las Srta. Myrian Alexandra Medina Tapia como requerimiento parcial a la obtención del título de Ingeniero en Sistemas e Informática.

Sangolquí, Julio de 2015

Ing. Carlos Montenegro
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Yo, Myrian Alexandra Medina Tapia declaro que la presente tesis de grado titulada "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", ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, de acuerdo a lo especificado en la bibliografía.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Julio de 2015

Myrian Alexandra Medina Tapia
C.I. 1303252421

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo, Myrian Alexandra Medina Tapia, autorizo a la Universidad de las Fuerzas Armadas – ESPE la publicación en la Biblioteca Virtual de la Institución del trabajo "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", cuyo contenido, ideas y criterio es de mi responsabilidad y autoría.

Sangolquí, Julio de 2015

Myrian Alexandra Medina Tapia
CI: 1303252421

AGRADECIMIENTO

A mis queridos padres Gonzalo y Myrian por su apoyo incondicional durante toda mi vida.

A mis hermanos y sobrinos por todo el cariño que siempre me han dado, en especial en los momentos difíciles.

Al Ingeniero Carlos Montenegro por respaldar mi tema de tesis y realizar las revisiones y observaciones de forma constante hasta la culminación de este interesante proyecto.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

De las investigaciones realizadas hasta el momento no existen estudios en el Ecuador sobre la complementariedad de las normas ISO/IEC 31000 e ISO/IEC 27005. Existe la necesidad de elaborar un estudio analítico que describa la gestión de riesgos en la seguridad de la información, los estándares ISO/IEC 31000 e ISO/27005, realice el análisis de compatibilidad y defina un esquema en integración entre las normas objeto de este estudio. Mediante la utilización de mapeos de alto nivel y detallados de estructuras, procesos, conceptos y anexos, se confirmó la factibilidad de lograr la integración de los estándares ISO/IEC 31000 e ISO/IEC 27005. El resultado obtenido determinó que la diferencia básica entre las normas es que la ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que la 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.

Palabras Clave:

- **ISO/IEC 31000**
- **ISO/IEC 27005**

ABSTRACT

Due to non-conclusive investigations in Ecuador regarding ISO/IEC 3100 and ISO/IEC 27005 IT Governance Security standards there is an imperative need for a formal study. This thesis 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.

Keywords:

- **ISO/IEC 31000**
- **ISO/IEC 27005**

CAPÍTULO 1
INTRODUCCIÓN

1.1 Planteamiento del Problema

De las investigaciones realizadas hasta el momento no existen estudios en el Ecuador sobre 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.

1.2 Objetivos

1.2.1 Objetivo General

Realizar un estudio analítico de la compatibilidad e integración de las normas ISO/IEC 31000 e ISO/IEC 27005 referente riesgos en la Seguridad de la Información.

1.2.2 Objetivos Específicos

a. Describir la situación actual de la gestión de riesgos en la Seguridad de la Información
b. Describir el estándar ISO/IEC 31000 (ISO, 2009)
c. Describir el estándar ISO/IEC 27005 (ISO, 2008)
d. Realizar el análisis de compatibilidad entre las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008)
e. Definir el esquema de integración entre las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008).

1.3 Justificación

Esta investigación es relevante porque generará un conocimiento que podrá ser utilizado por los tomadores de decisión de las organizaciones en lo relacionado a la gestión del riesgo y la implementación satisfactoria de esquemas de seguridad.

Todas las organizaciones grandes o pequeñas, se enfrentan a factores externos e internos que les quitan la certeza de alcanzar sus objetivos. Este efecto de falta de certeza es el "riesgo" y es inherente a todas las actividades, según Kevin W. Knight desarrollador del estándar ISO/IEC: 31000:2009. El riesgo es "el efecto de la incertidumbre en la consecución de los objetivos" ISO/IEC 31000 (ISO, 2009).

Las normas establecen un conjunto de principios que se deben satisfacer para que la gestión e implementación del riesgo sea eficaz y para que las organizaciones desarrollen, implementen y mejoren de manera continua un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.

Este problema de investigación podrá ser evaluado en varios niveles de la Organización y servirá de guía a los profesionales del sector de TI y a los líderes de las organizaciones en la Gestión del Riesgo enfocado 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.

1.4 Alcance

Este estudio describirá 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.

Se analizarán los beneficios y oportunidades de adoptar la Gestión del Riesgo como estrategia para alcanzar los objetivos y las metas.

CAPÍTULO 2
MARCO TEÓRICO

2.1 Riesgos en la Seguridad de la Información

2.1.1 Riesgo

El termino Gestión o Gerencia de Riesgos está definida en la Guía ISO/IEC 73, y se refiere al proceso de diseño, organización y coordinación de las actividades, como a la ejecución material de las mismas.

La guía ISO/IEC 73 indica que “El riesgo es definido como la combinación de la probabilidad de un suceso y sus consecuencias” (ISO, 2009). Los eventos que ocurren y el impacto que generar pueden ser oportunidades o amenazas a nivel empresarial. Los estándares consideran los riesgos como positivos y negativos, sin embargo a nivel de riesgos de seguridad, lo relevante es prevenir y mitigar el riesgo que hace daño.

2.1.2 Gestión de riesgos

La gestión de riesgos eficaz consiste en la identificación y tratamiento de los riesgos para maximizar el valor de las actividades de la empresa. La visualización de los factores negativos y positivos de los riesgos incrementa la probabilidad de éxito y reduce la probabilidad de fallo y la incertidumbre sobre la consecución de los objetivos generales de la empresa.

La gestión de riesgos es una disciplina orientada a empresas de cualquier tamaño y dedicadas a cualquier tipo de actividad de corto o largo plazo.

La gestión de riesgos es un proceso que se realiza de forma continua, constante y metódica en la estrategia de la empresa y en su aplicación; la cual se convierte en objetivos tácticos y operacionales, lo que implica la asignación de responsabilidades en todos los niveles de la empresa para lograr una mayor eficiencia. Las operaciones empresariales se ven afectadas por factores externos e internos a la organización tales como: financieros, operacionales, estratégicos, entre otros.

Figura 1. Contexto Gestión de Riesgos: Arquitectura de Riesgos, estrategia y protocolos

2.1.3 Proceso de Gestión de Riesgos

Valoración y Análisis de Riesgos

"La valoración de riesgos es el proceso general de análisis y evaluación de riesgos" (ISO, 2009), según lo indicado según la Guía ISO/IEC 73.

El análisis de riesgos comprende la identificación, descripción y estimación de riesgos.

Identificación de riesgos

Una empresa se desenvuelve en un entorno legal, social, político y cultural lo que implica que está expuesta a riesgos de todo tipo inclusive a amenazas internas y externas que pueden afectar el logro de los objetivos estratégicos y a su operación diaria. Para identificar estos riesgos es necesario conocer cuáles son los factores críticos para su éxito y las oportunidades relacionadas al logro de sus objetivos.

La identificación interna de los riesgos de las actividades relevantes de la organización a través de procesos y herramientas coordinadas entre sí, asegura que la gestión de riesgos sea propiedad de la empresa.

Las actividades y decisiones empresariales pueden ser estratégicas, operacionales, financieras, de gestión del conocimiento y de conformidad. Los objetivos estratégicos a largo plazo están condicionados a factores externos como riesgos políticos, cambios legales, disponibilidad de recursos económicos y la imagen de la empresa. Las actividades operacionales son aquellas diarias que permiten a la empresa lograr sus objetivos estratégicos.

El control financiero de la empresa y los efectos de factores externo como la disponibilidad de crédito, tipo de cambio de divisas, tipos de interés, son consideraras actividades financieras. El control de los recursos del conocimiento, la producción, protección y comunicación se relaciona a la gestión del conocimiento. Como ejemplo podemos mencionar el mal uso de la propiedad intelectual y la falla de los sistemas.

Las actividades de conformidad, están relacionadas a temas como salud y seguridad, medioambiente, protección del consumidor, protección de datos, prácticas de empleo y temas de regulación.

Descripción de riesgos

Describir los riesgos identificados de forma estructurada asegura un proceso de identificación, descripción y valoración de riesgos. La probabilidad de ocurrencias de riesgos considerados clave, permite priorizar y realizar un análisis exhaustivo de los mismos.

La identificación de los riesgos asociados a las actividades empresariales y la toma de decisiones se pueden calificar como estratégica, táctica u operacional. Es importante incorporar la gestión de riesgos en la fase de concepción de los proyectos así como a lo largo de la vida de un proyecto específico. A continuación se incluye como ejemplo una tabla que indica como describir y valorar los riesgos, para luego priorizar los mismos.

Tabla 1

Descripción de riesgos

Nombre del riesgo	Descripción del riesgo
Alcance del riesgo	Explicación detallada de eventos
Naturaleza del riesgo	Estratégicos, operacionales, financieros, gestión del conocimiento, etc.
Interesados	Logro de objetivos
Cuantificación del riesgo	Probabilidad de ocurrencia
Tolerancia del riesgo	Control del riesgo e impacto económico
Tratamiento del riesgo y herramientas de control	Métodos utilizados para controlar el riesgo
Reducir riesgos	Actividades a realizar
Definición política y estrategia	Responsable de ejecutar actividad

Estimación de riesgos

La estimación de riesgos puede ser cuantitativa, o cualitativa en términos de probabilidad de ocurrencia y de sus posibles consecuencias a nivel de riesgos, ya sean estos positivos o negativos. La probabilidad de que ocurra una oportunidad, puede ser alta (probable), media (posible) o

baja (remota), y su probabilidad de ocurrencia es de 75%, 25% al 75%, y de menos de 25% respectivamente.

En el caso de las amenazas, la probabilidad de ocurrencia varía de la siguiente manera: alta es más del 25%, media es menos del 25% y baja es de menos del 2%. A nivel de indicadores de tiempo, una amenaza de alta probabilidad puede ocurrir cada año, la media cada diez años, y la baja no sucede.

Perfil de riesgos

La creación de un perfil de riesgos valora cada riesgo y prioriza su tratamiento. Lo ubica en el área de la empresa que es afectada. Permite además aumentar el nivel de inversión para controlarlo en caso de requerirse.

Evaluación de riesgos

Una vez que los riesgos positivos y negativos son analizados, se realiza una comparación entre los riesgos definidos por la empresa y los riesgos estimados. La evaluación de riesgos nos permite determinar si debemos o no aceptar un riesgo específico; y determinar el nivel de costos en los que se puede incurrir y los beneficios a obtener, además de los requisitos legales, factores socioeconómicos y medioambientales.

Tratamiento de Riesgos

El tratamiento del riesgo permite seleccionar y aplicar medidas para modificar el riesgo, ya sea mitigándolo, eludiéndolo o transfiriéndolo, lo que implica asumir los costos económicos de hacerlo.

Las medidas de control interno son efectivas si los riesgos analizados son eliminados o reducidos. La rentabilidad depende de los beneficios obtenidos por la reducción de los riesgos si de adoptaron medidas de

control. Los costos de implementación permitirán medir la rentabilidad y también la pérdida sino se lo hace. Los resultados obtenidos deben ser analizados para ver si es conveniente el uso de las medidas de control.

Según los estándares internacionales, y de acuerdo a las leyes y regulaciones existentes una empresa debe tener un sistema de control de riesgos y debe financiar los riegos a través de seguros para evitar pérdidas.

Comunicación de Riesgos

El proceso de gestión de riesgos debe ser comunicado a los niveles directivos y a las unidades de negocio y a los inversionistas de la empresa. El consejo de administración de la empresa debe conocer cuáles son riesgos de mayor importancia y como estos afectan al valor de la empresa en el mercado, en relación a los rendimientos esperados. Los niveles directivos deben asegurar que el proceso de gestión de riesgos funciona correctamente para lo cual deben comunicar a toda la organización la política de riesgos y las responsabilidades inherentes a cada nivel.

Las diferentes áreas del negocio deben conocer sus responsabilidades en el proceso de gestión de riesgos, así como los impactos y las consecuencias que estos pueden provocar en otras áreas. Las herramientas de gestión que detecten variaciones en los presupuestos, les permiten tomar medidas oportunamente. La comunicación a los directivos de la empresa de los riesgos que se presenten o de errores que se detecten a través de las medidas de control establecidas es crítica.

Los individuos deben tomar conciencia de los riesgos individuales y además conocer cuál es su nivel de responsabilidad. El Consejo de administración debe asegurar que los controles de gestión adoptados funcionan adecuadamente e incluir en sus informes las obligaciones que tiene la dirección de la empresa sobre la gestión de riesgos, los procesos

utilizados para identificar los riesgos, los sistemas de control que existen y como estos son supervisados.

2.1.4 Administrar la gestión de riesgos

La política de gestión de riesgos debe indicar cuál es su orientación al riesgo, las responsabilidades de los interesados y los requisitos legales a nivel político, de seguridad y salud entre otros.

El proceso de gestión de riesgos para ser eficaz requiere el compromiso de la alta dirección, lo que implica la asignación de recursos que permitan disponer de herramientas y técnicas integradas entre sí que se utilizarán en las diferentes etapas del proceso. Es necesario que se defina una estructura que se encargue de administrar el proceso de gestión de riesgos que está formada por el Consejo de administración, las unidades de negocio y el gestor de riesgos.

El consejo de la Administración es el responsable de determinar la dirección estratégica de la empresa y de crear el entorno y las estructuras para que la gestión del riesgo sea eficaz. Entre varias de las funciones a su cargo están el análisis de los riesgos negativos, que hacer para minimizar su impacto y su probabilidad de ocurrencia, los costos y beneficios asociados al control de riesgos, y las consecuencias de las decisiones que se adopten.

Las unidades de negocio son las responsables de definir los objetivos de la gestión de riesgos en su operación diaria, analizar la exposición a los mismos, y de asegurar que se incorpore la gestión de riesgos en el ciclo de vida de los proyectos.

El gestor de riesgos debe realizar establecer la estrategia y la política de gestión de riesgos a nivel estratégico y operacional, crear las estructuras internas en las unidades de negocio, diseñar los procesos para el

tratamiento del riesgo, coordinar las actividades funcionales, desarrollar los planes de contingencia y elaborar los informes de riesgos.

La auditoría interna de una empresa u organización debe identificar y valorar los riesgos importantes, analizar y ser parte de los procesos de gestión de riesgos y capacitar al personal de operaciones en la gestión de riesgos y en el control interno.

La Empresa debe establecer los recursos necesarios para llevar a cabo la política de gestión de riesgos en todos los niveles de gestión y en cada unidad de negocios; y para integrarla a los procesos estratégicos, presupuestarios y operacionales. Las personas que son parte de la gestión de riesgos deben conocer cuáles son sus funciones en relación a la política y a la estrategia de gestión de riesgos. En el caso del área de auditoría, su función será la revisión de los controles internos.

2.1.5 Controlar el riesgo

La estructura interna que se crea para controlar el riesgo debe garantizar que los riesgos identificados sean tratados de acuerdo a las políticas establecidas, y controlados mediante auditorias continuas según lo indican los estándares.

Los cambios que se producen en las empresas debido al entorno en el que ocurren requieren que las actividades sean verificadas para asegurar que siguen los procedimientos definidos, ya que cualquier cambio puede significar modificaciones a los aplicativos. La información que se genere debe ser analizada y utilizada en el proceso de gestión de riesgos.

2.2 NORMA ISO/IEC 31000

La norma ISO 31000 (ISO, 2009) define principios para lograr que la gestión del riesgo sea eficaz. Considera además el establecimiento del contexto para determinar en qué entorno los objetivos de la organización se pueden lograr, las partes involucradas y los diferentes criterios de riesgo para evaluar su dificultad.

La implementación de la norma ISO 31000 (ISO, 2009) ayuda a la organización a identificar y a gestionar los riesgos y las políticas relacionadas a los mismos; a planificar sus actividades y a ser más eficientes en su operación, además de mejorar el aprendizaje y la flexibilidad de la organización a través de la introducción de controles y del uso adecuado de los recursos, lo que minimiza las pérdidas y la gestión de los incidentes.

2.2.1 Objeto

La ISO 31000 (ISO, 2009) es utilizada en todo tipo de organización para gestionar el riesgo, ya sea ésta una empresa privada o pública, asociaciones de individuos, y en cualquier tipo de industria durante todo el tiempo de vida de la misma en todas las actividades. Su campo de acción incluye estrategias, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

2.2.2 Términos y definiciones

Los términos utilizados en la norma ISO 31000 (ISO, 2009) son los siguientes:

Riesgo.- efecto de la incertidumbre sobre los objetivos.

Gestión del riesgo.- actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Marco de referencia para la gestión del riesgo.- entorno en el que se definen los criterios de una organización para diseñar, implementar, monitorear, revisar y mejorar de manera continua la gestión del riesgo.

Política para la gestión del riesgo.- directrices de la organización en relación a la gestión del riesgo.

Actitud hacia el riesgo.- postura que adopta la organización para evaluar, retener, tomar o alejarse del riesgo.

Plan para la gestión del riesgo.- esquema dentro del marco de referencia que especifica el enfoque, los componentes y los recursos que se van a aplicar a la gestión del riesgo.

Establecimiento del contexto.- definición de los parámetros internos y externos; y establecimiento del alcance y de los criterios del riesgo para la política de gestión del riesgo.

Contexto externo.- ambiente externo en el cual la organización se desenvuelve.

Contexto interno.- ambiente interno en el cual la organización logra sus objetivos.

Comunicación y consulta.- procesos continuos que una organización realiza para proveer, compartir u obtener información con las partes involucradas en relación a la gestión del riesgo.

Parte involucrada.- persona u organización que puede afectar, verse afectada o percibirse a sí misma afectada por una decisión o una actividad.

Valoración del riesgo.- proceso de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Identificación del riesgo.- proceso para encontrar, reconocer y describir el riesgo.

Fuente de riesgo.- elemento que tiene la capacidad de originar un riesgo.

Evento.- suceso que puede modificar un grupo de circunstancias.

Consecuencia.- resultado de un evento que afecta a los objetivos.

Probabilidad.- oportunidad de que algo suceda.

Perfil del riesgo.- descripción de un grupo de riesgos.

Análisis del riesgo.- proceso para determinar el nivel y la naturaleza del riesgo.

Criterios del riesgo.- términos de referencia en base a los cuales se evalúa el valor del riesgo.

Nivel del riesgo.- volumen del riesgo, identificado en base al análisis de las consecuencias y su probabilidad de ocurrencia.

Evaluación del riesgo.- Comparar el resultado del análisis del riesgo con los criterios del riesgo para determinar si el riesgo puede ser aceptado.

Tratamiento del riesgo.- proceso para modificar el riesgo.

Control.- medida que modifica el riesgo.

Riesgo residual.- restante después del tratamiento del riesgo.

Monitoreo.- verificación de un proceso para identificar cambios relacionados al nivel de ejecución esperada.

Revisión.- acción realizada, para identificar si algo es idóneo y eficaz para lograr un objetivo.

2.2.3 Principios

Los principios en los que se basa la norma ISO/IEC 31000 son:

1. Crear y proteger el valor de la organización.
2. Ser parte integral de todos los procesos de la organización.
3. Ser parte de la toma de decisiones
4. Abordar explícitamente la incertidumbre
5. Ser sistemática, estructurada y oportuna
6. Estar basada en la mejor información disponible
7. Estar adaptada al contexto externo e interno
8. Considerar los factores humanos y culturales de la organización
9. Ser transparente e inclusiva
10. Ser dinámica, reiterativa y receptiva al cambio
11. Facilitar la mejora continua de la organización

2.2.4 Marco de referencia

Generalidades

El marco de referencia para gestionar eficazmente el riesgo garantiza que la información que se genera permita tomar decisiones oportunas, y facilita la integración de la gestión del riesgo con la gestión de toda la organización. La gestión de riesgos se enfoca en evaluar cuales los riesgos significativos, y en aplicar respuestas adecuadas a estos riesgos.

Figura 2. Marco para la gestión del riesgo

Para reducir el nivel de incertidumbre asociado con el logro de los objetivos de la organización y la probabilidad de fallo, se requiere conocer el potencial de los factores de riesgo que pueden afectar a las actividades relevantes.

Dirección y Compromiso

El compromiso de la Dirección de la Organización y su participación en la gestión e implementación del riesgo y en la planificación estratégica garantizaría su eficacia. Uno de los elementos claves para lograrlo es alinear los objetivos estratégicos de la organización con los objetivos de la gestión del riesgo, al igual que utilizar indicadores de desempeño que midan los riegos en base a los indicadores de desempeño de la organización.

Diseño del Marco de Referencia

Entender el contexto externo e interno de una organización es un requisito previo al diseño e implementación del marco de referencia para la gestión del riesgo. Se considera contexto externo todo aquello relacionado al ambiente social, cultural, político, legal, reglamentario, financiero, tecnológico y económico de una organización y que afecta a sus objetivos, valores, percepciones, a nivel local, regional, nacional e inclusive internacional.

Antes de elaborar el marco de referencia es indispensable a nivel interno de la organización evaluar la estructura organizacional, las políticas, los objetivos, las estrategias, los recursos humanos, económicos y tecnológicos disponibles, y la cultura de la organización. Definir una política para la gestión del riesgo implica alinearse a los objetivos y a las políticas de la organización y considerar las obligaciones y responsabilidades para que la gestión del riesgo pueda ser realizada, comunicada y evaluada periódicamente.

La rendición de cuentas implica que la organización garantice y avale que los controles en el proceso de gestión de riesgos sean idóneos, eficaces y eficientes; a través de los propietarios del riesgo y de los responsables del diseño e implementación del marco de gestión, y de los individuos que son parte del proceso a nivel de toda la organización. La gestión del riesgo debe estar integrada a la planificación estratégica y del negocio, y a las prácticas de la gestión del cambio.

Implementar la Gestión del Riesgo

Implementar el marco de referencia implica que se defina el tiempo y la estrategia, que se aplique políticas y procesos que cumplan con normas reglamentadas y que se garantice que las decisiones adoptadas estén

alineadas con el proceso de gestión del riesgo a ser implementado, y consensuadas con los actores que participan en el mismo.

Monitorear y Revisar el Marco de Referencia

Monitorear la gestión del riesgo consiste en analizar los indicadores de gestión y los avances del plan de gestión del riesgo; y en verificar que el marco de referencia, la política y el plan para la gestión del riesgo siguen acordes al contexto interno y externo de la organización.

Mejora Continua del Marco de Referencia

Las decisiones adoptadas como consecuencia del monitoreo continuo del proceso antes indicado tendrán como resultado una mejora del marco de referencia, la política y el plan para la gestión del riesgo.

2.2.5 Proceso de Gestión del Riesgo

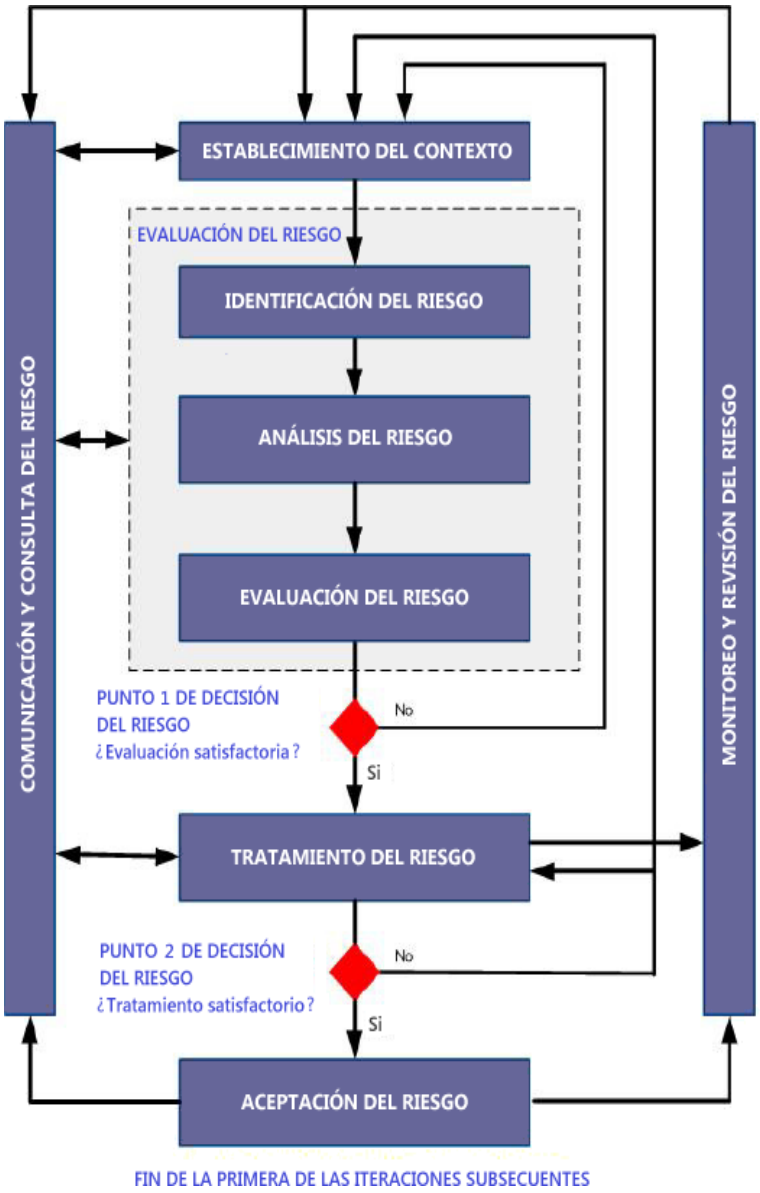

Figura 3. Proceso de Gestión del Riesgo

Comunicación y Consulta

La comunicación y la consulta se realizan durante todas las etapas del proceso de gestión del riesgo. Los planes de comunicación y consulta se hacen en las primeras etapas e incluyen las causas del riesgo, sus

consecuencias conocidas, y las medidas para tratarlo. Los responsables y los involucrados en la implementación del proceso deben conocer los motivos por los se adoptan las decisiones y se realizan las diferentes acciones.

Es necesario establecer el contexto, identificar los riesgos y considerar los intereses de las partes involucradas, y lograr la aprobación de los planes de tratamiento, y de comunicación y consulta externa e interna. Los criterios de los expertos en riesgos deben ser únicos en la definición y evaluación de los riesgos.

Establecimiento del Contexto

Establecer el contexto implica definir los objetivos, el alcance, y los parámetros externos e internos y los criterios que la organización utiliza para gestionar el riesgo.

El contexto externo incluye el relacionamiento con las partes externas a la organización y que le afectan en la consecución de sus objetivos; se desarrolla dentro de la organización y está relacionado a la estructura, políticas, objetivos, estrategias, cultura, recursos humanos, económicos, tecnológicos, sistemas de información, procesos, y normativa.

El contexto del proceso para la gestión del riesgo implica considerar las metas y los objetivos de las diferentes actividades y su alcance, y las responsabilidades asociadas a cada una de ellas; a más de los procesos, funciones, proyectos, servicios y sus relaciones con otros proyectos. La valoración del proceso de gestión del riesgo y su desempeño garantizaran que la gestión del riesgo es la apropiada para la organización.

La definición de los criterios para analizar el riesgo generalmente se la hace al inicio del proceso y pueden ser: la probabilidad, la temporalidad, el

nivel del riesgo y su tolerancia o aceptabilidad, la posibilidad de riesgos múltiples y la opinión de los involucrados en el proceso.

Valoración del Riesgo

La identificación, análisis y evaluación del riesgo constituyen la valoración del riesgo.

Identificación del Riesgo

Durante la etapa de la identificación del riesgo, se realiza un listado de los riesgos internos y externos que pueden afectar al logro de los objetivos de la organización y los eventos que los ocasionan. Es necesario conocer las causas, sus efectos y consecuencias y utilizar herramientas que ayuden en su identificación.

Análisis del Riesgo

Evaluar el riesgo implica que se definan parámetros de entrada, métodos y estrategias para analizar e identificar las causas y las fuentes que lo originan, y adoptar decisiones que probablemente generaran riesgos distintos.

El análisis de los riesgos implica determinar su probabilidad de ocurrencia y las consecuencias que pueden afectar el logro de objetivos. Al valorar los riesgos, es conveniente considerar los criterios que se usaron en su definición y la integración y dependencia que pudiera existir entre ellos.

El nivel del riesgo es una variable a tomar en cuenta; es todo lo que se ha asumido, y que debe ser comunicado a los interesados en el proceso, cuyas opiniones inclusive si son distintas unas de otras, deben ser establecidas. 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.

La probabilidad de ocurrencia de un riesgo se obtiene mediante la modelación de los resultados de uno o varios eventos, extrapolando los valores de los datos disponibles. El impacto de un riesgo en caso de ocurrir puede ser tangible o intangible.

Evaluación del Riesgo

Una vez que se analiza el riesgo, este debe ser evaluado en base a los resultados obtenidos para determinar el nivel de riesgo, los criterios definidos, y el tratamiento del mismo. En ciertos casos, la ocurrencia de un riesgo puede beneficiar a otras áreas de la organización, por lo cual se debe realizar un análisis exhaustivo del riesgo.

Tratamiento del Riesgo

Los riesgos pueden ser modificados si al ser evaluados se determinaron opciones que pueden reducir o eliminar su impacto. Tratar un riesgo implica analizar si el riesgo residual es tolerable, caso contrario se debe definir una nueva alternativa, cuyos resultados deben ser analizados. Se puede evitar el riesgo determinando que actividad lo origina.

Es posible que el riesgo aumente si se decide que es crítico lograr el objetivo propuesto. Si se elimina el origen del riesgo, su probabilidad de ocurrencia y sus consecuencias pueden variar. Los costos financieros de un riesgo compartido pueden ser asumidos por las áreas afectadas.

Selección de Opciones

Definir cuáles son las opciones más convenientes para el tratamiento del riesgo requiere equilibrar los costos y esfuerzos de la implementación versus los beneficios a ser obtenidos.

Es importante determinar cuáles son los riesgos graves que a pesar de tener una baja probabilidad, su tratamiento involucra un costo alto para la organización. En algunas ocasiones combinar las opciones para el tratamiento del riesgo es muy conveniente. Considerar las percepciones de los involucrados y la afectación que tiene el tratamiento del riesgo en otras áreas de la organización. Cuando se analiza un riesgo de forma individual definir el orden de prioridad es básico.

El plan de tratamiento del riesgo debe incluir los riesgos secundarios en todo el proceso.

Preparación e implementación de Planes

En esta etapa se documenta la selección de las opciones de tratamiento del riesgo, sus beneficios y su implementación, en base a un cronograma que incluya los responsables.

Monitoreo y Revisión

El proceso de monitoreo y revisión del riesgo valora el riesgo, analiza el contexto interno y externo, y verifica si existen cambios que afecten las opciones de tratamiento del riesgo definidas que impliquen una modificación de las mismas. Pueden presentarse riesgos emergentes que deben ser considerados.

En caso de utilizar indicadores de desempeño para tratar el riesgo y avances en la implementación, se incluirá la información que estos generen en el proceso de gestión de desempeño de la organización.

Registro del Proceso para la Gestión del Riesgo

Al realizar la trazabilidad del proceso de gestión del riesgo y sus actividades se debe definir cuál es la información sensible que se va a

almacenar en los registros y que beneficios se esperan obtener al hacerlo. Se debe considerar los costos de acceder, almacenar, recuperar y mantener estos registros y que tan fácil será hacerlo.

2.2.6 Atributos de la gestión mejorada del riesgo

Para realizar la gestión del riesgo las organizaciones deben considerar la criticidad de sus decisiones, para lo cual se definen algunos atributos e indicadores que muestran el nivel de desempeño en el proceso de la gestión del riesgo. Los atributos son la mejora continua, la rendición de cuentas y la aplicación de la gestión del riesgo en la toma de decisiones, comunicaciones continuas, Integración completa en la estructura de gobierno de la organización.

Mejora Continua

El proceso de mejora continua define indicadores que miden la existencia de metas explicitas de desempeño de gestión del riesgo, que permiten valorar y medir a la organización en su conjunto e individualmente. Esta valoración debe ser comunicada internamente y sus resultados revisados al menos anualmente, previo a la determinación de los objetivos de desempeño del siguiente año.

Rendición de Cuentas

Consiste en realizar actividades de control y monitoreo que traten el riesgo exhaustivamente. Estas actividades requieren de recursos para ser realizadas, y comunicadas a la organización; a más tener la jerarquía y autoridad necesaria para cumplir con sus objetivos.

Toma de Decisiones

La gestión del riesgo incluye una actividad que es la toma de decisiones, que es medida a través de un indicador que lleva un registro y de las decisiones adoptadas y su relación con el riesgo.

Comunicaciones Continuas

El desempeño de la gestión del riesgo y los reportes sobre los riesgos significativos debe ser comunicado continuamente a los involucrados dentro de la Organización. Las decisiones que se adopten se basan en la información recibida en relación al nivel del riesgo asumido y el tratamiento realizado para bajar su impacto.

Integración completa en la estructura de gobierno de la organización

La incertidumbre para lograr los objetivos en una organización constituyen los riesgos, El uso de indicadores es el lenguaje que utilizan los directivos para definir la no certeza del logro de un objetivo en las declaraciones de las políticas organizacionales y la documentación relacionada a la gestión del riesgo.

2.3 NORMA ISO/IEC 27005

La Norma ISO/IEC 27005 (ISO, 2008), fue preparada por el Comité Técnico de Tecnologías de la Información, ISO/IEC JTC 1, Subcomité SC 27, IT Security techniques.

Esta norma proporciona directrices para la gestión del riesgo de la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001 (ISO, 2005).

2.3.1 Objeto

Esta norma suministra directrices para la gestión del riesgo de la seguridad de la información y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

2.3.2 Referencias normativas

La norma ISO/IEC 27005 (ISO, 2008), utiliza para su aplicación a las normas ISO/IEC 27001 (ISO, 2005), Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos e ISO/IEC 27002 (ISO, 2005), Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

2.3.3 Términos y definiciones

En este documento se utilizan los términos y definiciones de la ISO/IEC 27001 (ISO, 2005) y la ISO/IEC 27002 (ISO, 2005).

2.3.4 Estructura de la norma

Esta norma contiene la descripción de los procesos para la gestión del riesgo de la seguridad de la información y sus actividades. Las actividades son: el establecimiento del contexto, la valoración, el tratamiento, la aceptación, la comunicación y el monitoreo y la revisión del riesgo. La estructura de cada actividad se define a continuación:

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.

2.3.5 Información general

El sistema de Gestión de Seguridad de la información está basado en un enfoque sistemático y sistémico enfocado en los procesos de negocios y en la gestión del riesgo de la empresa y su entorno.

La gestión del riesgo de la seguridad de la seguridad de la información identifica y valora los riesgos; informa su probabilidad de ocurrencia y sus consecuencias; monitorea y prioriza el tratamiento de los riesgos y las acciones para reducir su ocurrencia; comunica a los interesados y tomadores de decisión, y revisa continuamente el proceso de gestión y mitigación de riesgos.

2.3.6 Proceso de gestión del riesgo de la seguridad de la información

El proceso de gestión del riesgo de la seguridad de la información consta del establecimiento del contexto, la valoración del riesgo, el tratamiento del riesgo, la aceptación del riesgo, la comunicación del riesgo y el monitoreo y revisión del riesgo. La figura no. 3 muestra gráficamente el proceso de gestión del riesgo.

Las actividades de valoración y tratamiento del riesgo utilizan un enfoque iterativo para valorar las actividades y disminuir el tiempo y el esfuerzo en la identificación de los controles. Luego de establecer el contexto, se valora el riesgo una y otra vez y se definen las acciones necesarias para bajar los riesgos a un nivel aceptable. El contexto debe ser analizado al menos de forma parcial cada vez que se valora el riesgo.

Los riesgos residuales luego del tratamiento del riesgo no siempre son adecuados, en estos casos se debe repetir la valoración del riesgo, su aceptación y/o su impacto, y realizar nuevamente el tratamiento. La

aceptación del riesgo residual corresponde a los directores de la organización.

Las actividades del proceso de gestión de los riesgos deben ser comunicadas a las Autoridades y al personal involucrado en el mismo. La norma recomienda que se documente todas las actividades y los puntos de decisión del proceso de gestión del riesgo.

La norma ISO/IEC 27001 (ISO, 2005), indica que los controles que se ejecutan dentro del alcance, los límites y en el contexto del SGSI deben estar basados en el riesgo. Debido a esto se asocian las actividades del proceso de gestión del riesgo, con las fases de un SGSI.

TABLA 2

Alineamiento de un SGSI y el Proceso de Gestión del Riesgo en la Seguridad de la Información

Fase No.	Proceso del Sistema de Gestión de la Seguridad de Información	Proceso de Gestión del Riesgo en la seguridad de la Información
1	Planificar	Establecer el contexto, valorar el riesgo, planificar el tratamiento del riesgo y aceptación del riesgo
2	Hacer	Implementar el plan del tratamiento del riesgo
3	Verificar	Monitorear y revisar continuamente los riesgos detectados.
4	Actuar	Mantener y mejorar el proceso

2.3.7 Establecimiento del contexto

La estructura de la actividad Establecimiento del Contexto es la siguiente:

a) *Entrada:* la información que permita establecer el contexto en el que se encuentra la organización en relación a la gestión del riesgo.
b) *Acción*: definir los criterios básicos, el alcance, los límites y la estructura organizacional que realice la gestión del riesgo y establezca el contexto.

c) *Guía para la implementación*: dar soporte al SGSI y elaborar los planes de continuidad del negocio en caso de riesgos y de atención a incidentes.
d) *Salida:* especificar los criterios básicos, el alcance, los límites, y la descripción del proceso de gestión del riesgo.

Criterios Básicos

Dependiendo del alcance y los objetivos de la gestión del riesgo, se aplican enfoques diferentes que incluyan criterios de impacto, de evaluación y de aceptación del riesgo. La organización debe contar con los recursos necesarios para:

- Valorar el riesgo y establecer un plan de tratamiento del riesgo
- Definir e implementar políticas, procedimientos y controles
- Monitorear los controles y los procesos de gestión del riesgo.

Criterios de evaluación del riesgo

Al evaluar el riesgo se debe considerar cual es valor estratégico del negocio, que tan críticos son los activos de que dispone la empresa, cuales son los requisitos legales y las obligaciones contractuales, la disponibilidad, confidencialidad e integridad de la información en las operaciones del negocio y las expectativas y percepciones de las partes interesadas, a más de las consecuencias negativas para la imagen de la empresa.

Criterios de impacto

Los criterios de impacto del riesgo se definen en términos del daño que causen a la organización y de los costos que estos generen. Podemos mencionar los siguientes:

- Nivel de clasificación de los activos de información impactados
- Brechas de la seguridad de la información
- Operaciones deterioradas

- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños de la reputación de la empresa
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Criterios de la aceptación del riesgo

La organización define los criterios de aceptación del riesgo en base a políticas, metas y objetivos y establece escalas para los niveles de aceptación del riesgo. Los aspectos a ser considerados son:

- Definición de umbrales de riesgos múltiples
- La relación entre el beneficio y el riesgo estimado
- Aceptación de riesgos altos en caso de ser un requisito contractual
- Definición de requisitos para el tratamiento de riesgos futuros.

Cuando se analiza si un riesgo debe ser aceptado, es necesario considerar el negocio, las operaciones, las leyes, las finanzas, la tecnología y los factores sociales y humanitarios que se pueden ver afectados.

Alcance y Límites

La organización debe definir el alcance e identificar los límites de la gestión del riesgo de la seguridad de la información, realizar el análisis de los riesgos y valorar los activos críticos. Además se debe considerar lo siguiente:

- Políticas y estrategias de la organización
- Objetivos y procesos del negocio
- Funciones y estructura de la organización
- Requisitos legales, reglamentarios y contractuales
- Políticas de seguridad de la información
- Enfoque global de la organización hacia la gestión del riesgo

- Activos de información
- Ubicación de la organización y sus características geográficas
- Restricciones que afectan a la organización
- Expectativas de las partes interesadas
- Entorno sociocultural
- Intercambio de información con el entorno.

Proceso de Gestión del Riesgo

Los directivos de la organización deben aprobar el proceso de gestión del riesgo que se detalla a continuación:

- Desarrollar el proceso de gestión del riesgo de la seguridad de la información
- Identificar a los interesados
- Definir las funciones y las responsabilidades de las partes internas y externas
- Establecer las relaciones necesarias entre la organización y los interesados
- Definir las rutas para escalar decisiones
- Especificar los registros que se deben conservar.

2.3.8 Valoración del riesgo

La estructura de la actividad Valoración del Riesgo es la siguiente:

a) *Entrada:* se define el alcance, los límites y la estructura organizacional.

b) *Acción*: los riesgos se identifican, describen y priorizan de acuerdo a los objetivos de la organización.

c) *Guía para la implementación*: análisis, identificación, estimación y evaluación del riesgo. El valorar el riesgo implica identificar el riesgo

y determinar su probabilidad de ocurrencia; si esta es alta se el riesgo de ser evaluado de forma continua y exhaustiva.

d) *Salida:* los riesgos valorados y priorizados en base a los criterios de evaluación del riesgo.

Análisis del Riesgo

Identificación del Riesgo

El propósito de la identificación del riesgo es determinar que podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

A continuación se detallaran las actividades que son parte del análisis del riesgo.

Identificación de los Activos

La estructura de la actividad Identificación de los activos es la siguiente:

a) *Entrada*: alcance y límites del riesgo a ser valorado, lista de los componentes que incluyan la ubicación, funciones, y propietarios, etc.

b) *Acción:* Identificar los activos dentro del alcance establecido.

c) *Guía para la implementación*: Un activo tiene asignado un propietario el cual es quien puede determinar su valor en la organización y es responsable su buen uso y seguridad.

d) *Salida*: Listado de activos y de procesos del negocio asociados a los mismos.

Identificación de las Amenazas

La estructura de la actividad se detalla a continuación:

a) *Entrada:* listado de amenazas, usuarios, incidentes y los catálogos de amenazas externas.

b) *Acción:* identificar las amenazas y sus causas.

c) *Guía para la implementación*: las amenazas pueden causar daños a los activos de una organización tales como la información, los procesos y los sistemas. Las amenazas son de origen natural o humano, internas o externas a la organización y accidentales o deliberadas. Al valorar una amenaza se debe consultar el catálogo de amenazas y los incidentes ocurridos anteriormente.

d) *Salida*: listado de amenazas identificadas por tipo y origen.

Identificación de los Controles Existentes

La actividad tiene la siguiente estructura:

a) *Entrada:* listado de controles implementados para tratar el riesgo.

b) *Acción:* identificación de controles existentes y planificados.

c) *Guía para la implementación*: consiste en identificar los controles que existen y verificar su funcionamiento a través del SGSI. Si se determinen fallas se implementa controles adicionales. El control es eficaz si la probabilidad de ocurrencia de la amenaza disminuye, caso contrario es mejor eliminarlo o remplazarlo, dependiendo de su costo.

d) *Salida:* listado de controles implementados y su uso.

Identificación de las Vulnerabilidades

La estructura de la actividad se detalla a continuación:

a) *Entrada*: listado de amenazas conocidas, activos afectados y controles aplicados.

b) *Acción*: Identificar las vulnerabilidades que ocasionan que las amenazas afecten a los activos.

c) *Guía para la implementación*: se pueden identificar vulnerabilidades en las siguientes fases: organización, procesos y procedimientos, rutinas de gestión, personal, ambiente físico, configuración del sistema de información, hardware, software y equipo de comunicaciones.

d) *Salida:* listado de vulnerabilidades y su relación con los activos, las amenazas y los controles.

Identificación de las Consecuencias

La estructura de la actividad es la siguiente:

a) *Entrada:* listado de activos, procesos del negocio, amenazas y vulnerabilidades

b) *Acción:* identificación de las consecuencias como resultado de pérdidas de confidencialidad, integridad y disponibilidad de los activos.

c) *Guía para la implementación*: los incidentes producen consecuencias o daños en uno o varios activos. Un incidente describe una amenaza que explota una o varias vulnerabilidades. Se debe considerar el impacto cuando se establece el contexto. El valor del activo está determinado por el grado de afectación de la empresa ya sea de manera temporal o permanente.

d) Las consecuencias pueden ser ocasionadas por pérdida de tiempo de investigación y reparación del activo, pérdida de oportunidad y de tiempo, salud y seguridad, el costo financiero, imagen, reputación y buen nombre.

e) *Salida:* listado de posibles incidentes, consecuencias y los activos y procesos del negocio que pueden verse afectados.

Estimación del riesgo

Para realizar la estimación del riesgo se considera los criterios con los que se evaluaron los riesgos y se utilizan las metodologías cualitativas y las cuantitativas.

La estimación cualitativa identifica y evalúa los riesgos críticos y analiza el nivel del riesgo. Utiliza una escala de atributos que es definida de forma subjetiva y que permite determinar las consecuencias y su probabilidad de ocurrencia.

La estimación cuantitativa utiliza una escala de valores numéricos para analizar las consecuencias y su probabilidad de ocurrencia. Estos valores deben ser exactos para que puedan ser auditados. Su desventaja es que utiliza hechos históricos y no considera los riesgos nuevos.

Valoración de las consecuencias

La actividad "*Valoración de las Consecuencias"* tiene la siguiente estructura:

a) *Entrada**:*** listado de los incidentes, amenazas, vulnerabilidades, activos y procesos del negocio afectados.

b) *Acción*: evaluación del impacto de los incidentes y análisis de las consecuencias.

c) *Guías para la implementación*: el valor del impacto en el negocio se puede expresar de manera cualitativa y cuantitativa; sin embargo el asignar un valor monetario a los activos facilita la toma de decisiones. La extrapolación de los datos obtenidos como resultado de eventos ocurridos permite medir las consecuencias.

*d) Salida**:*** listado activos, criterios de impacto y consecuencias de un incidente.

Valoración de los incidentes

La estructura de la actividad "*Valoración de Incidentes*" se detalla a continuación:

a) *Entrada*: listado de incidentes, amenazas, activos afectados, vulnerabilidades explotadas, consecuencias a nivel de activos y procesos del negocio y controles existentes y planificados.

b) *Acción:* evaluar la probabilidad de ocurrencia de los incidentes.

c) *Guías para la implementación*: evaluar la probabilidad y el impacto de que ocurra un incidente utilizando técnicas de estimación cualitativas y cuantitativas y analizar la frecuencia y la probabilidad de ocurrencia de las amenazas accidentales o deliberadas; la vulnerabilidad de los activos y la eficacia de los controles.

d) *Salida:* probabilidad de ocurrencia de un incidente evaluada.

Nivel de estimación del riesgo

La estructura de la actividad se detalla a continuación:

a) *Entrada:* incidentes, consecuencias, activos y procesos de negocios, probabilidad de ocurrencia.

b) *Acción:* estimación del nivel de riesgo.

c) *Guía para la implementación*: evaluar las consecuencias de un riesgo, la probabilidad de ocurrencia de un incidente; y asignarles valores cualitativos o cuantitativos.

d) *Salida:* listado de riesgos estimados.

Evaluación del Riesgo

a) *Entrada**:*** una lista de los riesgos con los niveles de valor asignado y criterios para la evaluación del riesgo.

b) *Acción**:*** comparar los niveles de riesgo frente a los criterios para la evaluación y aceptación del riesgo

c) *Guía para la implementación*: los riesgos estimados y los criterios que se evaluaron para la toma de decisiones, deben compararse con el contexto definido para gestionar el riesgo, sin perder de vista los objetivos de la organización. Además el análisis del riesgo debe permitir tomar decisiones que garantices un nivel de riego aceptable. Los riesgos globales deben considerar la criticidad de los procesos del negocio.

d) *Salida**:*** listado de riesgos, prioridades, criterios de evaluación e incidentes que los puedan ocasionar.

2.3.9 Tratamiento del riesgo de la seguridad de la información

La estructura de la actividad "*Tratamiento del riesgo en la seguridad de la información*" es la siguiente:

a) *Entrada*: riesgos, prioridades, criterios de evaluación del riesgo, incidentes que puedan ocasionarlos.
b) *Acción**:*** seleccionar controles para reducir, retener, evitar o transferir los riesgos y elaborar un plan para el tratamiento del riesgo.
c) *Guía para la implementación*: las opciones para tratar el riesgo son: la reducción de la probabilidad de los riesgos y de sus consecuencias; y la transferencia o retención de los riesgos residuales. La elaboración del plan del tratamiento del riesgo, requiere definir prioridades cuando se establecen los riesgos a ser analizados y utilizar técnicas para clasificar el riesgo, y el análisis del

costo-beneficio. Para establecer los riesgos residuales, se debe valorar el riesgo luego de tratarlo, hasta lograr la aceptación por parte de la organización.

d) *Salida*: plan para el tratamiento del riesgo y riesgos residuales.

En la figura no. 4, se puede visualizar la actividad para el tratamiento del riesgo y los procesos que la componen.

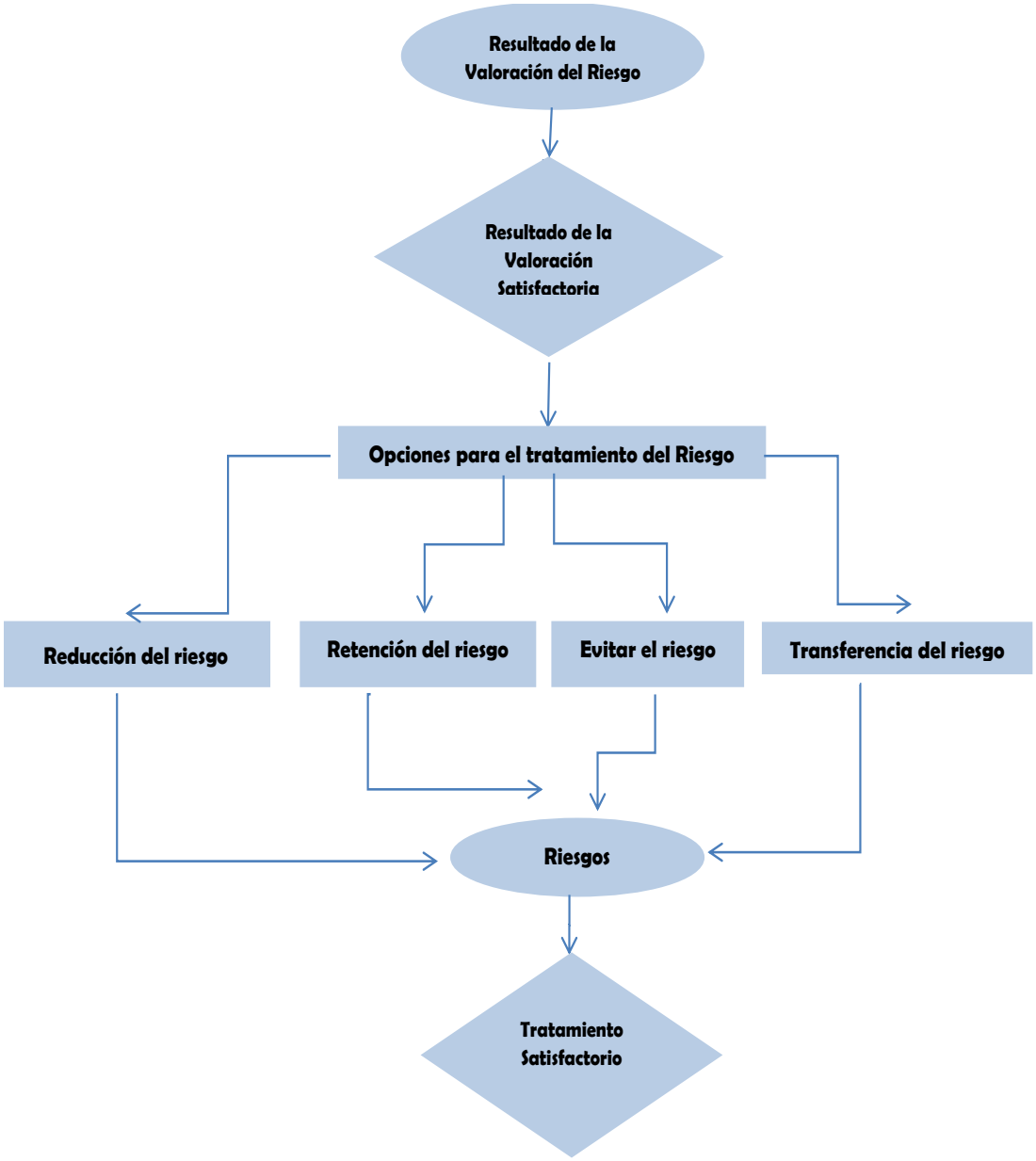

Figura 4. Actividad para el tratamiento del riesgo

A continuación se detallaran las estructuras de todas las actividades que forman parte del tratamiento del riesgo.

Reducción del Riesgo

a) *Acción**:*** Reducir el nivel del riesgo mediante la selección de controles hasta obtener el riesgo residual aceptable.

*b) Guía para la implementación**:***

a. Disminuir costo total de propiedad del sistema con controles que incluyan criterios de aceptación del riesgo, costos, tiempo de implementación, aspectos técnicos, ambientales y culturales
b. Definir costos de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles y compararlos con el valor del activo que se protege
c. Analizar el retorno de la inversión en términos de reducción del riesgo
d. Analizar las restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, de personal, de integración de controles nuevos y existentes y facilidad de uso
e. Identificar una solución que garantice la seguridad de la información. Asegurar que las restricciones de carácter técnico implementadas a través de un control no afecten el desempeño.

c) *Salida**:*** Controles posibles, costos, beneficios y prioridades de implementación.

Retención del Riesgo

a) *Acción**:*** evaluar el riesgo y decidir si se lo debe mantener.

b) *Guía para la implementación*: analizar los criterios de aceptación del riesgo, y retenerlo sin implementar controles adicionales.

Evitar el Riesgo

a) *Acción:* evitar la acción que da origen al riesgo particular.

b) *Guía para la implementación*: analizar el impacto del riesgo y el costo de implementar el tratamiento versus el beneficio a obtener y decidir si se evita el riesgo modificando las actividades o las condiciones bajo las cuales se efectúan.

Transferir el Riesgo

a) *Acción*: transferir el riesgo en base a su evaluación.

b) *Guía para la implementación*: Al transferir un riesgo podemos crear nuevos o modificar los actuales, esto implica que los riesgos se vuelvan a tratar. Para evitar que el sistema de información sufra ataques, se debe monitorear constantemente. La gestión del riesgo puede ser transferida a un tercero sin embargo, el impacto en caso de producirse sigue siendo responsabilidad de la organización.

2.3.10 Aceptación del riesgo de la seguridad de la información

a) *Entrada:* plan para el tratamiento del riesgo y valoración del riesgo residual.

b) *Acción:* Aceptar los riesgos, definir y registrar responsabilidades.

c) *Guía para la implementación*:

a. definir la forma de tratar el riesgo valorado en el plan de tratamiento considerando los criterios de aceptación establecidos.

b. Analizar y aprobar el plan de tratamiento del riesgo, los riesgos residuales y las condiciones de aceptación establecidas para su aprobación.

c. Analizar si el riesgo residual cumple los criterios de aceptación del riesgo y si circunstancias prevalentes fueron tomadas en cuenta. Si no se lo hizo, hay que justificarlo indicando el alto costo de reducir el riesgo y el beneficio a ser obtenido

d. Revisar oportunamente los criterios de aceptación del riesgo previo a aceptar y justificar el riesgo.

d) *Salida:* Riesgos aceptados y justificados.

2.3.11 Comunicación de los riesgos de la seguridad de la información

A continuación se detallan las estructuras de la actividad:

a) *Entrada**:*** información del riesgo resultado de la gestión del mismo.

b) *Acción**:*** intercambiar y compartir la información entre los tomadores de decisión y las partes involucradas

c) *Guía para la implementación*:

a. Comunicar el riesgo de forma oportuna entre los tomadores de decisión y las partes involucradas que les permita gestionar el riesgo y decidir qué acciones que se deben ejecutar para eliminar las brechas de seguridad y evitar incidentes.

b. Intercambiar información sobre la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.
c. Analizar la forma en que los interesados perciben el riesgo. Cuando se aceptan riesgos por la forma en que estos se perciben, es conveniente documentar cual fue el motivo y que beneficios se piensan obtener
d. Presentar el plan para el tratamiento del riesgo.

d) *Salida**:*** La gestión del riesgo es entendida por los interesados.

2.3.12 Monitoreo y revisión del riesgo de la seguridad de la información

A continuación se detalla las estructura de cada una de las actividades que componen el Monitoreo y la revisión del riesgo.

Factores de Riesgo

a) *Entrada**:*** actividades de gestión del riesgo.

b) *Acción**:*** analizar oportunamente y de forma continua el contexto y los cambios que se produzcan en los factores de riesgos, como son el valor de los activos, las amenazas, los incidentes y la probabilidad de ocurrencia, para mantener controlado el riesgo.

c) *Guía para la implementación*: debido a que el riesgo es dinámico debe ser controlado y monitoreado de forma continua. Si se detecta cambios en el valor de los activos existentes o recién adquiridos, que pueden ser vulnerables a amenazas y cuya probabilidad de ocurrencia sea alta, se debe revisar si las opciones seleccionadas para tratar el riesgo son adecuadas. Para identificar que el riesgo tenga un nivel aceptable, se debe adoptar medidas de control como

agrupar los riesgos bajos y aceptados y evaluar su impacto potencial acumulado.

d) *Salida*: La vinculación constante entre los objetivos del negocio y los objetivos de la gestión del riesgo, a más de los criterios de aceptación.

Gestión del Riesgo

a) *Entrada**:*** Actividades de gestión del riesgo

b) *Acción**:*** Chequear de forma sistemática el proceso de gestión del riesgo

c) *Guía para la implementación*:

   a. Revisar los resultados de valorar y tratar el riesgo y la vigencia de la gestión del riesgo y los planes de gestión de forma continua.
   b. Informar a las autoridades involucradas y a los interesados de las mejoras en el proceso de gestión del riesgo que ayuden en la toma de decisiones.
   c. Analizar la validez de los criterios utilizados para valorar los riesgos, los cuales deben estar acordes a las estrategias del negocio y a los cambios en el contexto legal, ambiental y de mercado. Los criterios a ser revisados son de: impacto, evaluación y aceptación del riesgo.
   d. Disponer de recursos económicos para el monitoreo de la gestión del riesgo.
   e. Detectar cambios que modifiquen el objeto del proceso de la gestión del riesgo.

d) *Salida**:*** Adaptar continuamente el proceso de la gestión riesgo de la seguridad de información a los objetivos del negocio.

CAPÍTULO 3

ESTUDIO ANALÍTICO

La Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC) han publicado los siguientes estándares para el manejo de los riesgos y la seguridad de la información:

- ISO/IEC 31000 (ISO, 2009), Gestión de Riesgos – Principios y Guías;
- ISO/IEC 31010 (ISO, 2009), Gestión de Riesgos – Técnicas de Evaluación de Riesgos;
- ISO/IEC 27001 (ISO, 2005), Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27005 (ISO, 2008), Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de Riesgos en la Seguridad de la Información.

Se procede a realizar un análisis general de las normas ISO/IEC 31000 (ISO, 2009), Gestión de Riesgos – Principios y Guías e ISO/IEC 27005 (ISO, 2008), Tecnologías de la información – Técnicas de Seguridad – Sistemas de Gestión de Riesgos en la Seguridad de la Información, que permitirá determinar los parámetros que deben seleccionarse para comparar ambas normas.

3.1 Descripción de Parámetros de Comparación

A continuación se describirá brevemente las características generales de las normas ISO/IEC 31000 (ISO, 2009) y ISO/IEC 27005 (ISO, 2008):

Tabla 3

Características Generales Normas ISO 31000 e ISO 27005

Características	ISO/IEC 31000	ISO/IEC 27005
Propietario	Organización Internacional de Publicación de Estándares	Organización Internacional de Publicación de Estándares
País de Origen	Suiza	Suiza
Mercado Objetivo	Organización de cualquier tamaño, actividad o sector.	Gobierno, agencias, Grandes empresas y pymes
Nombre	La ISO 31000:20009, *Principios y Guías para la Gestión de Riesgos*.	La ISO/IEC 27005, *Guías para la gestión del riesgo de la seguridad de la información.*
Objetivo	ISO 31000 es una familia de normas relativas a la gestión de riesgos según la Organización Internacional de Normalización.	ISO 27005 pertenece al grupo de los estándares de la serie 27000 que cubre la información de la gestión de riesgos en la seguridad de la información.
Fecha de Publicación	ISO 31000 fue publicada como norma el 13 de noviembre de 2009, al igual que la Guía ISO/IEC 73.	ISO 27005 fue publicada en junio de 2008. En 2011, ISO lanzó una nueva versión de la norma.
Remplazó a:	ISO 31000: 2009 reemplazo a la norma vigente en la gestión de riesgos, AS / NZS 4360: 2004.	ISO 27005 sustituyó a la Gestión de la Información y Comunicaciones Tecnología de Seguridad, la norma ISO / IEC TR 13335-3:1998 y la norma ISO / IEC TR 13335-4:2000.
Descripción	El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices genéricas sobre la gestión de riesgos. A más de proporcionar un estándar sobre la aplicación de la gestión de riesgos. Define el riesgo como "efecto de la incertidumbre en los objetivos" y se aplica a todo tipo de riesgo, sin considerar su naturaleza y sus consecuencias. No es específica para alguna industria o sector. Y se utiliza en actividades estratégicas, operacionales y de gestión organizacional. ISO 31000:2009 aborda el riesgo de la siguiente manera: evitándolo al no continuar con una actividad, asumiéndolo para lograr un objetivo, eliminándolo, modificando su probabilidad de ocurrencia y sus consecuencias. *La norma ISO 31000 no recomienda un sistema de clasificación de riesgos específico.* *La ISO 31000 enumera las principales ventajas de una Organización Internacional de publicación de estándares.*	El estándar ISO 27005 ayuda a las organizaciones en determinar cómo y porqué gestionar los riesgos *en la seguridad de la información*, para apoyar los objetivos de gobernabilidad. Soporta los requerimientos de seguridad de un sistema de seguridad de información, según lo establecido por la ISO 27001. Es aplicable a todo tipo de organización pública, privada y sin fines de lucro en la gestión de los riesgos. ISO 27005 consta de 55 páginas. Este estándar soporta los conceptos generales especificados en la ISO/IEC 27001 y está diseñada para guiar y soportar la implementación de la seguridad de la información efectiva basada en un enfoque en el manejo de riesgos. Estándar internacional que apoya la tarea del Análisis y la gestión de riesgos en el marco de un Sistema de Gestión de la Seguridad de la Información. La ISO 27005 permite desarrollar criterios para la evaluación del riesgo, para lo cual se considera el valor estratégico del proceso de información, la importancia de la disponibilidad y confidencialidad de la información y las expectativas y percepciones de las partes interesadas.

La estructura de las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008), se describe a continuación:

Tabla 4

Estructura de las Normas

ESTRUCTURA	ISO 31000	ISO 27005
Principios	La norma define once principios que una organización debe cumplir para gestionar el riesgo. 1. Crea y protege el valor y contribuye al logro de los objetivos y la mejora de rendimiento 2. Es parte integral de los procesos de la organización. No es una actividad autónoma e independiente 3. Es parte de la toma de decisiones 4. Aborda explícitamente la incertidumbre, su naturaleza y la forma en que se puede abordar 5. Es sistemática, estructurada y oportuna y conduce a la eficiencia y a resultados consistentes, comparables y fiables 6. Se basa en la mejor información disponible 7. Se adapta al contexto, a los riesgos externos e internos y al perfil del riesgo. 8. Considera factores humanos y culturales e involucra a los interesados en todos los niveles. 9. Es transparente e inclusiva 10. Es dinámico, interactivo y sensible a los cambios 11. Facilita la mejora continua de la organización, la cual debe mejorar su grado de madurez en la gestión de riesgos. *La ISO 31000 no explica en forma detallada la forma en la cual los principios deben aplicarse en la organización.*	La ISO 27005 es una guía que sirve para gestionar los riesgos de la seguridad de la información, de acuerdo a los principios definidos en otras normas de la serie 27000. *Los principios a los que se adapta la norma ISO 27005 son definidos en otras normas de la serie 27000.*
Marco de trabajo	El Marco de trabajo analiza la necesidad de integrar la gestión del riesgo en los procesos de gestión de la organización, alinearla a los objetivos y la cultura de la organización y proporcionar los recursos adecuados para apoyar la gestión de los riesgos. (Cláusula 4) El marco de trabajo de la ISO 31000 se compone de: 1. Mandato y Compromiso de la Junta 2. Diseño del Marco de Trabajo 3. Implementar la Gestión de Riesgos 4. Revisión y monitoreo del Marco de Trabajo 5. Mejorar el Marco de Trabajo *ISO 31000 describe un marco para implementar la gestión del riesgo, no para administrarlo.* *La información sobre el diseño del marco que apoya el proceso de gestión de riesgos no es establecido en detalle en la norma ISO 31000.*	Establecimiento del contexto. (Cláusula 7)
Procesos	Describe 5 actividades: 1. Comunicación y consulta 2. Establecimiento del contexto 3. Evaluación de riesgos 4. Tratamiento del riesgo 5. Monitoreo y revisión del riesgo *Los principales componentes de ambas normas a nivel de procesos son muy similares y se complementan entre sí.*	Define 7 actividades: 1. Visión general del proceso de gestión de riesgo de la seguridad 2. Establecimiento del contexto 3. Valoración del riesgo de la seguridad de la información 4. Tratamiento del riesgo de la *seguridad de la información* 5. Aceptación del riesgo en la *seguridad de la información* 6. Comunicación de los riesgos de la *seguridad de la información* 7. Monitoreo y revisión del riesgo *de la seguridad de la información.*

Continúa →

Procesos	**1.** ***Comunicación y consulta*** Se realiza con grupos de interés internos y externos durante todas las etapas del proceso.	
	2. Establecimiento del contexto Articula sus objetivos, define los parámetros y establece el ámbito de aplicación. Se requiere una estructura para sostener e implementar el proceso de gestión del riesgo. ISO 31000 se refiere a esta estructura como el contexto de la gestión del riesgo.	
	2. ***Evaluacion*** Incluye la identificación, análisis y evaluación de riesgos. Se elabora una lista de todos los riesgos y se los analiza para entender las causas y las fuentes de riesgos, las consecuencias y la probabilidad de ocurrencia. Se evalúa el proceso de toma de decisiones en base a la comparación de los criterios que se usaron para determinar el riesgo.	
	2. ***Tratamiento del riesgo*** Selecciona y aplica opciones para modificar riesgos y compara los costes y esfuerzos versus los beneficios y desarrolla e implementa planes de tratamiento del riesgo.	
	5.Monitoreo y revisión Evaluación de la eficacia, la obtención de nueva información, la identificación de nuevos riesgos y realiza una grabación del proceso para proporcionar la trazabilidad y bases para mejorarlo.	
ANEXOS	**Incluye 1 anexo:** Anexo A, Atributos de mejora de la gestión de riesgos, se refiere al desarrollo de un adecuado nivel de desempeño en la gestión de riesgos. Los atributos son los siguientes: a) La mejora continua a través del establecimiento de metas de desempeño b) La responsabilidad completa para los involucrados c) La aplicación en todas las comunicaciones continuas de toma de decisiones d) Plena integración en la estructura de gobierno de la organización. *La ISO 31000 menciona la aplicación del desempeño organizacional sin embargo no incluye ninguna guía para hacerlo.*	**Incluye 6 anexos:** Anexo A, Definición del alcance y los límites del proceso de gestión del riesgo de la seguridad de la información. Anexo B, Identificación y valoración de los activos y valoración del impacto Anexo C, Ejemplos de amenazas comunes. Anexo D, Vulnerabilidades y métodos para la valoración de la vulnerabilidad. Anexo E, Enfoques para la valoración de riesgos de la información. Anexo F, Restricciones para la reducción de riesgos.
Certificación	La norma no puede ser usada para propósitos de certificación y acreditación.	La norma no puede ser usada para propósitos de certificación y acreditación.

3.2 Selección y Aplicación de Parámetros de Comparación

Del análisis realizado previamente se ha estimado que los parámetros que deben ser seleccionados entre las normas ISO/IEC 31000 (ISO, 2009)

e ISO/IEC 27005 (ISO, 2008), son: la estructura de las normas, los procesos básicos, los conceptos y los anexos.

3.2.1 Comparación de Procesos Básicos

A continuación se detallan los procesos similares de ambas normas:

Tabla 5

Procesos - Normas ISO/IEC 31000 e ISO/IEC 27005

ISO 27005	ISO 31000
Establecimiento del Contexto	Establecimiento del Contexto
Identificación del Riesgo	Identificación del Riesgo
Análisis del Riesgo	Análisis del Riesgo
Evaluación del Riesgo	Evaluación del Riesgo
Tratamiento del Riesgo	Tratamiento del Riesgo
Monitoreo y Revisión	Monitoreo y Revisión
Comunicación y Consulta	Comunicación y Consulta

Al analizar los procesos de la gestión del riesgo en las normas ISO/IEC 27005 (ISO, 2008) e ISO/IEC 31000 (ISO, 2009) se determina que los aspectos comunes en ambas normas, en relación a las actividades son los siguientes:

Tabla 6

Aspectos Comunes - Normas ISO/IEC 27005 e ISO/IEC 31000

Procesos Básicos		Aspectos Comunes ISO 27005 e ISO 31000
Establecimiento del Contexto	a)	Se establece una visión/contexto de los riesgos de TI teniendo en cuenta las partes involucradas desde arriba hacia abajo
	b)	Se definen los criterios de evaluación de los riesgos
	c)	Se alinea el proceso con los objetivos de la empresa
Identificación del riesgo	a)	Se define el universo completo de los riesgos existentes
	b)	Se establecen escenarios de riesgo
	c)	Se identifican los riesgos con mayor posibilidad
	d)	Se identifican las consecuencias
Análisis del riesgo	a)	Se evalúa los controles existentes
	b)	Se define el método de evaluación de riesgos
	c)	Se estima el nivel de riesgo
Evaluación del riesgo	a)	Se evalúa el impacto y probabilidad de cada riesgo
	b)	Se interpreta y se documenta el resultado de la evaluación
Tratamiento del riesgo	a)	Se definen las estrategias para tratamiento de los riesgos
	b)	Se preparan e implementan los planes de acción
Monitoreo y revisión	a)	Se evalúa los cambios constantes en el contexto externo e interno y los factores de riesgos y como estos afectan al proceso de la gestión de riesgos
Comunicación y Consulta	a)	Se define un plan de comunicaciones claro involucrando todos los interesados del proceso de gestión de riesgos.

3.2.2 Mapeo de Procesos de Alto Nivel

Al realizar el análisis de los procesos de la gestión del riesgo de las normas ISO/IEC 27005 (ISO, 2008) e ISO/IEC 31000 (ISO, 2009), se determinó que existe integración y que en todos ellos se realizan actividades similares en el proceso de ejecución de las normas, motivo por el cual se realizó un mapeo de alto nivel que se detalla a continuación:

Tabla 7

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)

Al realizar el análisis del nivel de coincidencia en los procesos de alto nivel, se 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 relación.

3.2.3 Mapeo detallado ISO/IEC 31000 a ISO/IEC 27005

Tabla 8

Mapeo detallado ISO/IEC 31000 a ISO/IEC 2005

	ISO/IEC 31000		ISO/IEC 27005	Nivel de Coincidencia
	TÉRMINOS			"+"
3	PRINCIPIOS			"-"
4	MARCO DE REFERENCIA			
4.a	*Generalidades*			"-"
4.b	*Dirección y Compromiso*			"-"
4.c	Diseño del marco de referencia			"-"
4.d	Implementar la gestión del riesgo			"-"
4.d1	*Implementar el marco de referencia*			"-"
4.d2	*Implementar el proceso de la gestión del riesgo*			"-"
4.e	Monitorear y revisar el marco de referencia			"-"
4.f	Mejora continua del marco de referencia			"-"
5	PROCESO		PROCESO	
5.a	Generalidades		Visión General del proceso	"+"
5.b	Comunicación y Consulta	11	Comunicación de los riesgos	"+"
5.c	Establecimiento del contexto	7	Establecimiento del Contexto	"+"
		7.1	*Consideraciones Generales*	"o"
		7.2	*Criterios básicos*	"o"
		7.3	*El alcance y los límites*	"o"
		7.4	*Organización para la gestión del riesgo*	"o"
5.d	Valoración del riesgo	8	Evaluación del Riesgo	"+"
		8.1	*Descripción de la valoración del riesgo*	"-"
5.d1	*Identificación del riesgo*	8.2.1	*Identificación del riesgo*	"+"
5.d2	*Análisis del riesgo*	8.2	*Análisis del riesgo*	"+"
		8.2.2	*Estimación del riesgo*	"+"
5.d3	*Evaluación del riesgo*	8.3	*Evaluación del riesgo*	"+"
5.e	Tratamiento del riesgo	9	Tratamiento del riesgo	"+"
5.e1	*Selección de opciones*	9.1	*Descripción general*	"+"
5.e2	*Preparación e implementación de planes*	9.2	*Reducción del riesgo*	"o"
		9.3	*Retención del riesgo*	"o"
		9.4	*Evadir el riesgo*	"o"
		9.5	*Transferencia del riesgo*	"o"
		10	Aceptación del riesgo en la seguridad de la información	"-"
5.f	Monitoreo y Revisión	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*	"+"
5.g	Registro del Proceso para la gestión del Riesgo			"-"

(+) Coincidencia Significativa (14)

(0) Coincidencia menor (8)

(-) Enfoque menor o no relacionado (12)

A realizar el análisis de coincidencia de la estructura de ambas normas, se determinó que existen, 14 "+" coincidencias significativas, 8 "o" coincidencias menores y 12 "-"actividades no relacionadas entre sí, lo que indica que de un total de 34 opciones, solo 12 no tienen relación entre sí.

3.2.4 Mapeo de Conceptos ISO/IEC 31000 e ISO/IEC 27005

En la siguiente tabla se realiza una comparación de los términos que se utilizan en ambas normas objeto del estudio. Básicamente se analiza la norma o guía que lo originó, la diferencia en caso de existir, y el nivel de coincidencia.

Tabla 9

Mapeo de Conceptos

Término	ISO 31000 Definición (origen ISO Guía 73:2009)	ISO 27005:2008 Definición (origen ISO/IEC 27001 y/o ISO/IEC 27002)	Diferencia	Nivel de Coincidencia
Activo		Cualquier cosa que tiene valor para la organización y que por eso requiere protección.	La norma ISO 27005, realiza una identificación y valoración de los activos en el Anexo B1 y B2.	"-"
Consecuencia	Resultado de un evento que afecta a los objetivos. *[ISO/IEC Guía 73:2009]*	ISO/IEC 27005:2011 Resultado de un evento que afecta a los objetivos. *[ISO/IEC Guía 73:2009]*		"+"
Control	Es una medida que modifica el riesgo. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Mide el riesgo que ha sido modificado. [ISO/IEC Guía 73:2009] Las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.	Ambas normas utilizan el mismo el término proveniente de la Guía ISO 73.	"+"

Continúa →

Evento	Suceso que puede modificar un grupo particular de circunstancias. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Suceso que puede modificar un grupo particular de circunstancias. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Contexto interno	Ambiente interno, en el que la organización busca alcanzar sus objetivos. [ISO/IEC Guía 73:2009	ISO/IEC 27005:2011 Ambiente interno, en el que la organización busca alcanzar sus objetivos. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Contexto externo	Ambiente externo en el cual la organización se desenvuelve. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Entorno externo en el cual la organización se desenvuelve. [ISO/IEC Guía 73:2009]	Las últimas versiones de las ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Riesgo	Efecto de la incertidumbre en los objetivos. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2008 Combinación de la probabilidad de un evento y su consecuencia ISO/IEC 27005:2011 Efecto de la incertidumbre en los objetivos. [ISO/IEC Guía 73:2009]	La ISO 27005:2008 utiliza un concepto distinto sin embargo en su versión del 2011, el riesgo proviene de la Guía ISO 73 al igual que la ISO 31000.	"+"
Nivel del riesgo	Volumen del riesgo, identificado en base al análisis de las consecuencias y su probabilidad de ocurrencia. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Magnitud del riesgo expresada en términos de la combinación de consecuencias y su probabilidad. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Probabilidad	Oportunidad de que algo suceda. ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Oportunidad de que algo suceda ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Riesgo residual	Riesgo que queda después del tratamiento del riesgo. [ISO/IEC Guía 73:2009]	El riesgo remanente luego de una amenaza a la seguridad. ISO/IEC 27005:2011, Riesgo que queda después del tratamiento del riesgo. [ISO/IEC Guía 73:2009]	La ISO 27005:2008 utiliza un concepto distinto sin embargo en su versión del 2011, el riesgo residual proviene de la Guía ISO 73 al igual que en la ISO 31000.	"+"
Análisis del riesgo	Proceso para determinar el nivel y la naturaleza del riesgo. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2008 Uso sistemático de la información para identificar fuentes y estimar riesgo. ISO/IEC 27005:2011 Proceso para determinar el nivel y la naturaleza del riesgo. [ISO/IEC Guía 73:2009]	La ISO 27005:2008 utiliza un concepto distinto sin embargo en su versión del 2011, el análisis del riesgo proviene de la Guía ISO 73 al igual que en la ISO 31000.	"+"
Valoración del riesgo	Proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2008 Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado significativo del riesgo. ISO/IEC 27005:2011 Proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos. [ISO/IEC Guía 73:2009]	La ISO 27005:2008 utiliza un concepto distinto sin embargo en su versión del 2011, la valoración del riesgo proviene de la Guía ISO 73 al igual que en la ISO 31000.	"+"

Continúa →

Comunicación y consulta	Procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73	"+"
Criterios del riesgo	Términos de referencia en base a los cuales se evalúa el valor del riesgo. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Términos de referencia en base a los cuales se evalúa el valor del riesgo [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas utilizan el término proveniente de la Guía ISO 73.	"+"
Evaluación del riesgo	Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable y tolerable. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable y tolerable. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas, utilizan el término especificado en la Guía ISO 73.	"+"
Identificación del riesgo	Proceso para encontrar, reconocer y describir el riesgo. [ISO/IEC Guía 73:2009]	Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. ISO/IEC 27005:2011 Proceso de encontrar, reconocer y describir los riesgos. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas, utilizan el término especificado en la Guía ISO 73.	"+"
Gestión del Riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas, utilizan el concepto especificado en la Guía ISO 73.	"+"
Tratamiento del riesgo	Proceso para modificar el riesgo. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2008 Proceso de selección e implementación de mediciones para modificar el riesgo. ISO/IEC 27005:2011 Proceso para modificar el riesgo. [ISO/IEC Guía 73:2009]	La ISO 27005:2008 utiliza un concepto distinto sin embargo en su versión del 2011, el tratamiento del riesgo proviene de la Guía ISO 73 al igual que en la ISO 31000.	"+"
Interesado	Persona u organización que puede afectar, verse afectada o percibirse a sí misma afectada por una decisión o una actividad. [ISO/IEC Guía 73:2009]	ISO/IEC 27005:2011 Persona u organización que puede afectar, ser afectada o percibirse a sí misma afectada por una decisión o actividad. [ISO/IEC Guía 73:2009]	Las últimas versiones de ambas normas, utilizan el concepto especificado en la Guía ISO 73.	"+"
Establecer el contexto en la Gestión de Riesgos de la Información	Definición de los parámetros internos y externos y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.	Definir los criterios básicos necesarios para la gestión de riesgos de seguridad de la información (ISO / IEC 27005 7.2). Definir el alcance y los límites (ISO / IEC 27005 7.3). Establecer una organización adecuada para gestionar los riesgos en seguridad de la información (ISO / IEC 27005 7.4.)	ISO/IEC 31000 se orienta a la gestión de riesgos de forma general, no así la ISO/IEC 27005 que lo hace de forma específica a la gestión de riesgos en la seguridad de la información.	"+"

Continúa →

Impacto		n/a	ISO/IEC 27005:2011 Cambio adverso en el nivel de los objetivos del negocio logrados. [ISO/IEC Guía 73:2009]	La ISO 27005 valora el impacto en los activos, en el anexo B3.	"-"
Riesgo en la seguridad de la información		n/a	ISO/IEC 27005:2011 Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. [ISO/IEC Guía 73:2009]	La ISO 31000 no trata de forma específica el riesgo en la seguridad de la información, sino el riesgo en forma general.	"-"
Evitación del riesgo		n/a	ISO/IEC 27005:2011 Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. [ISO/IEC Guía 73:2009]		"-"
Comunicación del riesgo		n/a	ISO/IEC 27005:2011 Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas. [ISO/IEC Guía 73:2009]		"-"
Estimación del riesgo		n/a	ISO/IEC 27005:2011 Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. [ISO/IEC Guía 73:2009]		"-"
Reducción del riesgo		n/a	ISO/IEC 27005:2011 Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. [ISO/IEC Guía 73:2002]		"-"
Retención del riesgo		n/a	ISO/IEC 27005:2011 Aceptación de la pérdida o ganancia proveniente de un riesgo particular. [ISO/IEC Guía 73:2009]		"-"
Transferencia del Riesgo		n/a	ISO/IEC 27005:2011 Compartir con otra de las partes la pérdida o la ganancia de un riesgo.[ISO/IEC Guía 73:2009]		"-"
Fuente de riesgo	Elemento que tiene la capacidad de originar un riesgo.		n/a		"-"
Perfil del riesgo	Descripción de un grupo de riesgos.		n/a		"-"
Política para la gestión del riesgo	Directrices de la organización en relación a la gestión del riesgo.				"-"
Actitud hacia el riesgo	Postura que adopta la organización para evaluar, retener, tomar o alejarse del riesgo.		n/a		"-"
Plan para la gestión del riesgo	Esquema dentro del marco de referencia que especifica el enfoque, los componentes y los recursos que se van a aplicar a la gestión del riesgo.		n/a		"-"
Monitoreo	Verificación de un proceso para identificar cambios relacionados al nivel de ejecución esperada.		n/a		"-"

Continúa →

Revisión	Acción realizada, para identificar si algo es idóneo y eficaz para lograr un objetivo.	n/a	"-"
Marco de referencia para la gestión del riesgo	Entorno en el que se definen los criterios de una organización para diseñar, implementar, monitorear, revisar y mejorar de manera continua, la gestión del riesgo.	n/a	"-"

(+) Coincidencia Significativa (19)

(0) Coincidencia menor (0)

(-) Enfoque menor o no relacionado (17)

A realizar el análisis del mapeo detallado de conceptos, se determinó que existen, 19 "+" procesos que tienen coincidencias significativa, 0 "o" coincidencias menores y 17 "-" actividades no relacionadas entre sí.

Los conceptos utilizados en las normas ISO/IEC 31000 e ISO/IEC 27005 (ISO, 2011), provienen de la Guía ISO 73 (ISO, 2009), lo que se refleja en las coincidencias significativas. Sin embargo en los 17 casos donde no existe relación, implica que los conceptos en la versión de la ISO 27005 (ISO, 2008) su alcance era distinto.

Cabe mencionar que la versión de la norma ISO/IEC 27005 (ISO, 2008) objeto de este estudio es la del año 2008, que es la disponible en el mercado ecuatoriano a través del INEN.

3.2.5 Mapeo de Anexos ISO/IEC 31000 e ISO/IEC 27005

En la tabla 10 se realiza un análisis del contenido de los anexos que utilizan las normas ISO/IEC 31000 e ISO/IEC 27005. Además se determina si existe un nivel de coincidencia o complementariedad entre ellos.

Tabla 10

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, si considera las comunicaciones continuas con los interesados, la integración con la organización a nivel de riesgos y el análisis o valoración de los riesgos constante.	"+"
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*** • **Estudio de la Organización** • **Restricciones que afectan a la Organización** • **Referencias legislativas y reglamentarias que afectan a la organización** • **Restricciones que afectan el alcance.**	**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* Permite desarrollar evaluaciones de pérdidas basado en impactos operacionales directos e indirectos.		"-"
Norma ISO / IEC 27005 Anexo B	n/a	*Comparación de impactos operacionales directos.* La operación se puede ver afectada por: • El valor de reposición financiera de pérdidas parciales de activos • El costo de adquisición, configuración e instalación de un activo • El costo de las operaciones suspendidas debido al incidente que afecto un activo • La violación de la seguridad de la información.		"-"

Continúa →

ISO / IEC 27005 Anexo B	n/a	*Impactos operacionales indirectos* • El costo de oportunidad, que implica los recursos financieros requeridos para reemplazar un activo • El costo de la interrupción de las operaciones • Uso indebido de la información debido a brechas de seguridad • Violación de obligaciones legales • Violación de códigos de conducta.		"-"
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* Tipos de Vulnerabilidades: 1. Hardware 2. Software 3. Red 4. Personal 5. Lugar 6. Organización Métodos de valoración: 1. Herramienta automática de exploración de la vulnerabilidad 2. Prueba y evaluación de la seguridad 3. Pruebas de penetración 4. Revisión de código.	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. • Valoración de alto nivel de riesgos • Valoración detallada de los riesgos.	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 hace describe las restricciones relacionadas a la reducción del riesgo.	"-"

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

A realizar el análisis del mapeo de los anexos de las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008), se encontró que existen 6 "-" anexos que no tienen relación entre sí. Existe una coincidencia que se ha considerado significativa, en relación al Anexo A, de la norma ISO 31000 (ISO, 2009) con la norma 27005 (ISO, 2008) a nivel de procesos.

El mapeo de anexos indica, y que es el Anexo A de la ISO/IEC 31000 (ISO, 2009), tiene una coincidencia significa, ya que a pesar de que no muestra relación con los otros anexos, si lo hace a nivel general con información que se encuentra en otros procesos de 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.

CAPÍTULO 4

RESULTADOS DEL ESTUDIO ANALÍTICO

4.1. Presentación de resultados de la compatibilidad e integración

4.1.1 Integración de Procesos de las Normas ISO 31000 e ISO 27005

Se ha considerado realizar una integración a nivel de procesos entre las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 2700 (ISO, 2008), objeto de este estudio. Los procesos seleccionados son los siguientes:

a) Comunicación y Consulta
b) Establecimiento del Contexto
c) Valoración del Riesgo
d) Tratamiento del Riesgo
e) Monitoreo y Revisión del Riesgo.

La descripción de cada uno los procesos, se realizará más adelante en este documento.

4.1.2 Integración de Conceptos de las Normas ISO 31000 e ISO 27005

En la siguiente tabla se ha unificado los conceptos que utilizan las normas ISO 31000 (ISO, 2009) e ISO 27005 (ISO, 2008), que permitirá constatar la complementariedad existente, a nivel de origen, contenido y aplicación.

Tabla 11

Integración de Conceptos

Término	ISO 31000 e ISO 27005:20011 (origen ISO Guía 73:2009) ISO 27005:2008 (origen ISO/IEC 27001 y/o ISO/IEC 27002)
Activo	**Cualquier cosa que tiene valor para la organización y que por eso requiere protección. [ISO/IEC 27001 y/o ISO/IEC 27002]**
Consecuencia	ISO/IEC 27005:2011 + ISO/IEC 31000 Resultado de un evento que afecta a los objetivos. [origen ISO/IEC Guía 73:2009]
Control	ISO/IEC 27005:2011 + ISO/IEC 31000 Mide el riesgo que ha sido modificado. [origen ISO/IEC Guía 73:2009]
Evento	ISO/IEC 27005:2011 + ISO/IEC 31000 Suceso que puede modificar un grupo particular de circunstancias [origen ISO/IEC Guía 73:2009]
Contexto interno	ISO/IEC 27005:2011 + ISO/IEC 31000 Ambiente interno, en el que la organización busca alcanzar sus objetivos. [origen ISO/IEC Guía 73:2009]
Contexto externo	ISO/IEC 27005:2011 + ISO/IEC 31000 Ambiente externo en el cual la organización se desenvuelve. [origen ISO/IEC Guía 73:2009]
Riesgo	ISO/IEC 27005:2011 + ISO/IEC 31000 Efecto de la incertidumbre en los objetivos. [origen ISO/IEC Guía 73:2009] ISO/IEC 27005:2008 Combinación de la probabilidad de un evento y su consecuencia.
Nivel del riesgo	ISO/IEC 27005:2011 Magnitud del riesgo expresada en términos de la combinación de consecuencias y su probabilidad. [origen ISO/IEC Guía 73:2009]
Análisis del riesgo	ISO/IEC 27005:2011 + ISO/IEC 31000 Proceso para determinar el nivel y la naturaleza del riesgo. [origen ISO/IEC Guía 73:2009] ISO/IEC 27005:2008 Uso sistemático de la información para identificar fuentes y estimar riesgo.
Valoración del riesgo	ISO/IEC 27005:2011 + ISO/IEC 31000 Proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos. [origen ISO/IEC Guía 73:2009]. ISO/IEC 27005:2008 Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado significativo del riesgo.
Comunicación y consulta	Procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo. [origen: ISO/IEC Guía 73:2009]
Criterios del riesgo	Términos de referencia en base a los cuales se evalúa el valor del riesgo.[origen: *ISO/IEC Guía 73:2009*]
Evaluación del riesgo	Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable y tolerable. *[origen ISO/IEC Guía 73:2009]*
Identificación del riesgo	Proceso para encontrar, reconocer y describir el riesgo.*[origen: ISO/IEC Guía 73:2009]* Proceso para encontrar, enumerar y caracterizar los elementos del riesgo. *[origen: ISO/IEC Guía 73:2002]*
Gestión del Riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. *[origen: ISO/IEC Guía 73:2009]*
Tratamiento del riesgo	ISO/IEC 27005:2008 Proceso de selección e implementación de mediciones para modificar el riesgo. *[origen: ISO/IEC 27001 e ISO/IEC 27002]* ISO/IEC 27005:2011 Proceso para modificar el riesgo. *[origen: ISO/IEC Guía 73:2009]*
Interesado	Persona u organización que puede afectar, verse afectada o percibirse a sí misma afectada por una decisión o una actividad. *[origen: ISO/IEC Guía 73:2009]*

Continúa →

Establecer el contexto en la Gestión de Riesgos de la Información	Definición de los parámetros internos y externos y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. *[ISO/IEC Guía 73:2009]* ISO / IEC 27005:2008 • Definir los criterios básicos necesarios para la gestión de riesgos de seguridad de la información. • Definir el alcance y los límites. • Establecer una organización adecuada para gestionar los riesgos en seguridad de la información *[origen: ISO/IEC 27001 y/o ISO/IEC 27002]*
Establecer el contexto en la Gestión de Riesgos de la Información **Impacto**	Definición de los parámetros internos y externos y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. *[ISO/IEC Guía 73:2009]* ISO / IEC 27005:2008 • Definir los criterios básicos necesarios para la gestión de riesgos de seguridad de la información. • Definir el alcance y los límites. • Establecer una organización adecuada para gestionar los riesgos en seguridad de la información *[origen: ISO/IEC 27001 y/o ISO/IEC 27002]* ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Cambio adverso en el nivel de los objetivos del negocio logrados. *[origen: ISO/IEC Guía 73:2009]*
Riesgo en la seguridad de la información	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. *[origen: ISO/IEC Guía 73:2009]*
Evitar el riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. *[origen: ISO/IEC Guía 73:2009 y Guía 73:2002]*
Comunicación del riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas. *[origen: ISO/IEC Guía 73:2009 y Guía 73:2002]*
Estimación del riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. *[origen: ISO/IEC Guía 73:2009 y Guía 73:2002]*
Reducción del riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. *[origen: ISO/IEC Guía 73:2009 y Guía 73:2002]*
Retención del riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Aceptación de la pérdida o ganancia proveniente de un riesgo particular. *[origen: ISO/IEC Guía 73:2009 y Guía 73:2002]*
Transferencia del Riesgo	ISO/IEC 27005:2011 e ISO/IEC 27005:2008 Compartir con otra de las partes la pérdida o la ganancia de un riesgo. [origen: *ISO/IEC Guía 73:2009 y Guía 73:2002]*
Fuente de riesgo	Elemento que tiene la capacidad de originar un riesgo. *[origen: ISO/IEC Guía 73:2009]*
Perfil del riesgo	Descripción de un grupo de riesgos. *[origen: ISO/IEC Guía 73:2009]*
Política para la gestión del riesgo	Directrices de la organización en relación a la gestión del riesgo. *[origen: ISO/IEC Guía 73:2009]*
Actitud hacia el riesgo	Postura que adopta la organización para evaluar, retener, tomar o alejarse del riesgo. *[ISO/IEC Guía 73:2009]*
Plan para la gestión del riesgo	Esquema dentro del marco de referencia que especifica el enfoque, los componentes y los recursos que se van a aplicar a la gestión del riesgo. *[ISO/IEC Guía 73:2009]*
Monitoreo	Verificación de un proceso para identificar cambios relacionados al nivel de ejecución esperada. *[ISO/IEC Guía 73:2009]*
Revisión	Acción realizada, para identificar si algo es idóneo y eficaz para lograr un objetivo. *[ISO/IEC Guía 73:2009]*
Marco de referencia para la gestión del riesgo	Entorno en el que se definen los criterios de una organización para diseñar, implementar, Monitorear, revisar y mejorar de forma continua la gestión del riesgo. *[origen: ISO/IEC Guía 73:2009]*

Como se especificó en la tabla, el origen de los conceptos de la norma ISO 27005 (ISO, 2008) son las normas ISO 27001 (ISO, 2005) e ISO 27002 (ISO, 2005) y en algunos casos la guía ISO 73:2002. Las normas ISO 31000 (ISO, 2009) e ISO 27005 (ISO, 2011) utilizan la terminología de la Guía 73:2009.

4.1.3 Integración de Anexos de las Normas ISO/IEC 31000 e ISO/IEC 27005

A continuación se detallan los anexos que utilizan las normas objeto del estudio:

Tabla 12

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 de las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008), 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 norma ISO/IEC 27005 (ISO, 2008), en cambio baja de nivel y se orienta a definir el alcance del proceso, y entra de lleno en 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.

4.2 Discusión de resultados

Como se ha demostrado en el desarrollo del trabajo es factible integrar las normas ISO/IEC 31000 (ISO, 2009) e ISO/IEC 27005 (ISO, 2008) entre sí, para lograr que una Organización alcance sus objetivos, debido a la complementariedad y aproximación existente entre ambas, lo que se ve reflejado en el mapeo de alto nivel y específico de sus estructuras, procesos, conceptos, términos y anexos realizado en el capítulo anterior.

Finalmente, gracias a la consistencia del análisis es posible elaborar un documento que servirá de base para “Gestionar los riesgos en la seguridad de la información en base a las normas ISO/IEC 31000 e ISO/IEC 27005” y que se detalla a continuación.

4.2.1 Integración de las Normas ISO/IEC 31000 e ISO/IEC 27005

Objeto

La integración de las normas ISO 31000 (ISO, 2009) e ISO 27005 (ISO, 2008) puede ser utilizada por cualquier organización de carácter público o privada para gestionar el riesgo en la seguridad de la información a nivel de estrategias, operaciones, proyectos, procesos, productos y servicios.

Términos y Definiciones

A continuación se detallan los términos utilizando en las normas ISO/IEC 31000 e ISO/IEC 27005:

Activo.- Cualquier cosa que tiene valor para la organización y que por eso requiere protección.

Consecuencia.- Resultado que afecta a los objetivos.

Control.- Mide el riesgo que ha sido modificado.

Evento.- Suceso que puede modificar un grupo particular de circunstancias.

Contexto interno.- Ambiente interno, en el que la organización busca alcanzar sus objetivos.

Contexto externo.- Ambiente externo en el cual la organización se desenvuelve.

Riesgo.- Efecto de la incertidumbre en los objetivos y/o Combinación de la probabilidad de un evento y su consecuencia.

Nivel del riesgo.- Magnitud del riesgo expresada en términos de la combinación de consecuencias y su probabilidad.

Análisis del riesgo.- Proceso para determinar el nivel y la naturaleza del riesgo y/o Uso sistemático de la información para identificar fuentes y estimar riesgo.

Valoración del riesgo.- Proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos y/o Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado significativo del riesgo.

Comunicación y Consulta.- Procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener

información, y para entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo.

Criterios del riesgo.- Términos de referencia en base a los cuales se evalúa el valor del riesgo.

Evaluación del riesgo.- Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable y tolerable.

Identificación de riesgo.- Proceso para encontrar, reconocer y describir el riesgo.

Gestión del Riesgo.- Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Tratamiento del Riesgo.- Proceso para modificar el riesgo y/o Proceso de selección e implementación de mediciones para modificar el riesgo.

Interesado.- Persona u organización que puede afectar, verse afectada o percibirse a sí misma afectada por una decisión o una actividad.

Establecer el contexto en la Gestión de Riesgos de la Información.- Definición de los parámetros internos y externos; y establecimiento del alcance y de los criterios y las políticas de gestión del riesgo.

Impacto.- Cambio adverso en el nivel de los objetivos del negocio logrados.

Riesgo en la seguridad de la información.- Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Evitar el riesgo.- Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Comunicación del riesgo.- Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

Estimación del riesgo.- Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Reducción del riesgo.- Acciones que se toman para disminuir la probabilidad de las consecuencias negativas o ambas, asociadas con un riesgo.

Retención del riesgo.- Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Transferencia del riesgo.- Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Fuente de riesgo.- Elemento que tiene la capacidad de originar un riesgo.

Perfil del riesgo.- Descripción de un grupo de riesgos.

Política para la gestión del riesgo.- Directrices de la organización en relación a la gestión del riesgo.

Actitud hacia el riesgo.- Postura que adopta la organización para evaluar, retener, tomar o alejarse del riesgo.

Plan para la gestión del riesgo.- Esquema dentro del marco de referencia que especifica el enfoque, los componentes y los recursos que se van a aplicar a la gestión del riesgo.

Monitoreo.- Verificación de un proceso para identificar cambios relacionados al nivel de ejecución esperada.

Revisión.- Acción realizada para identificar si algo es idóneo y eficaz para lograr un objetivo.

Marco de referencia para la gestión del riesgo.- Entorno en el que se definen los criterios de una organización para diseñar, implementar, monitorear, revisar y mejorar de forma continua la gestión del riesgo.

Principios

1. Crear y proteger el valor de la organización.
2. Ser parte integral de todos los procesos de la organización.
3. Ser parte de la toma de decisiones
4. Abordar explícitamente la incertidumbre
5. Ser sistemática, estructurada y oportuna
6. Estar basada en la mejor información disponible
7. Estar adaptada al contexto externo e interno
8. Considerar los factores humanos y culturales de la organización
9. Ser transparente e inclusiva
10. Ser dinámica, reiterativa y receptiva al cambio
11. Facilitar la mejora continua de la organización.

Marco de Referencia

Generalidades

El marco de referencia logra que la información que se genera permita tomar decisiones oportunas relacionadas con la gestión e integración del riesgo a nivel de toda la organización. Proporcionada además los recursos necesarios para hacerlo.

La gestión de riesgos se enfoca en evaluar cuales los riesgos significativos, y en aplicar respuestas adecuadas a estos riesgos. Para reducir el nivel de incertidumbre asociado con el logro de los objetivos organizacionales y la probabilidad de fallo, se requiere conocer el potencial de los factores de riesgo que pueden afectar a las actividades relevantes.

Dirección y compromiso

El compromiso de la Dirección de la Organización, su participación en la gestión e implementación del riesgo y en la planificación estratégica

garantiza su eficacia. Para conseguirlo es indispensable alinear los objetivos estratégicos de la organización con los objetivos de la gestión del riesgo, y utilizar indicadores de desempeño que midan los riesgos, basados en los indicadores de desempeño que utiliza la organización.

Diseño del Marco de referencia

Entender el contexto externo e interno de una organización es un requisito previo al diseño e implementación del marco de referencia para la gestión del riesgo. Se considera contexto externo todo aquello relacionado al ambiente social, cultural, político, legal, reglamentario, financiero, tecnológico y económico de una organización y que afecta a sus objetivos, valores, percepciones, a nivel local, regional, nacional e inclusive internacional.

Antes de elaborar el marco de referencia es indispensable a nivel interno de la organización evaluar la estructura organizacional, las políticas, los objetivos, las estrategias, los recursos humanos, económicos y tecnológicos disponibles, y la cultura de la organización.

Definir una política para la gestión del riesgo implica alinearse a los objetivos y a las políticas de la organización y considerar las obligaciones y responsabilidades para que la gestión del riesgo pueda ser realizada, comunicada y evaluada periódicamente.

La rendición de cuentas implica que la organización garantice y avale que los controles en el proceso de gestión de riesgos sean idóneos, eficaces y eficientes; a través de los propietarios del riesgo y de los responsables del diseño e implementación del marco de gestión, y de los individuos que son parte del proceso a nivel organizacional.

La gestión del riesgo debe estar integrada a la planificación estratégica y del negocio, y a las prácticas de la gestión del cambio.

Implementar la gestión del riesgo

Implementar el marco de referencia implica que se defina el tiempo y la estrategia, que se aplique políticas y procesos que cumplan con normas reglamentadas y que se garantice que las decisiones adoptadas estén alineadas con los procesos de gestión del riesgo y consensuadas con los actores que participan en el mismo. Adicionalmente se debe implementar el proceso para la gestión del riesgo.

Monitorear y revisar el marco de referencia

Monitorear la gestión del riesgo consiste en analizar los indicadores de gestión y los avances del plan de gestión del riesgo; y en verificar que el marco de referencia, la política y el plan para la gestión del riesgo siguen acordes al contexto interno y externo de la organización.

Mejora continua del marco de referencia

Las decisiones adoptadas como consecuencia del monitoreo continuo del proceso, tendrán como resultado una mejora del marco de referencia, la política y el plan para la gestión del riesgo.

Procesos

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: el establecimiento del contexto, la valoración, el tratamiento, la aceptación, la comunicación y consulta, y el monitoreo y la revisión del riesgo, lo que se puede apreciar en la figura No. 3 del Proceso de Gestión del Riesgo. 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. La estructura de esta actividad es la siguiente:

a) ***Entrada:*** información del riesgo resultado de la gestión del mismo.

b) ***Acción:*** intercambiar y compartir información entre los tomadores de decisión y las partes involucradas.

c) ***Guía de implementación***:

   a. Comunicar el riesgo de forma oportuna entre los tomadores de decisión y las partes involucradas que les permita gestionar el riesgo y decidir qué acciones que se deben ejecutar para eliminar las brechas de seguridad y evitar incidentes
   b. Intercambiar información sobre la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos
   c. Analizar la forma en que los interesados perciben el riesgo que fueron aceptados y documentar los motivos y los beneficios que se esperan obtener
   d. Presentar el plan para el tratamiento del riesgo.

d) ***Salida:*** La gestión del riesgo es entendida por los interesados.

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. La estructura de la actividad es la siguiente:

a) ***Entrada:*** la información que permita establecer el contexto en el que se encuentra la organización respecto a la gestión del riesgo.

b) ***Acción:*** definir los criterios básicos, el alcance, los límites y la estructura organizacional a cargo de gestionar el riesgo y establecer el contexto.
c) ***Guía de implementación***: elaborar los planes de continuidad del negocio en caso de riesgos y de atención a incidentes.
d) ***Salida:*** especificar los criterios básicos, el alcance, los límites, y la descripción del proceso de gestión del 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.

a) ***Entrada:*** se define el alcance, los límites y la estructura organizacional.

b) ***Acción***: los riesgos se identifican, describen y priorizan de acuerdo a los objetivos de la organización.

c) ***Guía para la implementación***: análisis, identificación, estimación y evaluación del riesgo. Valorar el riesgo implica identificarlo y determinar su probabilidad de ocurrencia; si esta es alta, el riesgo de ser evaluado de forma continua y exhaustiva.

d) ***Salida***: los riesgos valorados y priorizados en base a los criterios de evaluación del 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.

Identificación de Activos

a) ***Entrada:*** alcance y límites del riesgo a ser valorado, lista de los componentes con sus propietarios, ubicación, funciones, etc.

b) ***Acción***: Identificar los activos dentro del alcance establecido.

c) ***Guía para la implementación***: Un activo tiene asignado un propietario el cual es quien puede determinar su valor en la organización y es responsable de su buen uso y seguridad.

d) ***Salida***: Listado de activos y procesos del negocio asociados a los mismos.

Identificación de Amenazas

a) ***Entrada:*** listado de amenazas, usuarios, incidentes y catálogos de amenazas externas.

b) ***Acción***: identificar las amenazas y sus causas.

c) Guía para la implementación: las amenazas pueden causar daños a los activos de una organización tales como la información, los procesos y los sistemas. Las amenazas son de origen natural o humano, internas o externas a la organización y accidentales o deliberadas. Al valorar una amenaza se debe consultar el catálogo de amenazas y los incidentes ocurridos anteriormente.

d) ***Salida***: listado de amenazas identificadas por tipo y origen.

Identificación de Controles existentes

a) ***Entrada***: listado de controles implementados para tratar el riesgo.

b) ***Acción***: identificar los controles existentes y los planificados.

c) ***Guía para la implementación***: consiste en identificar los controles que existen y verificar su funcionamiento a través del SGSI. Si se determinen fallas en su funcionamiento se implementa controles adicionales. Si la probabilidad de ocurrencia de la amenaza no disminuye se debe eliminar o remplazar el control, previo análisis de su costo.

d) Salida: listado de controles implementados y su uso.

Identificación de Vulnerabilidades

a) ***Entrada:*** listado de amenazas conocidas, activos afectados y controles aplicados

b) ***Acción:*** Identificar las vulnerabilidades que ocasionan que las amenazas afecten a los activos.

c) ***Guía para la implementación***: se identifican vulnerabilidades en las fases de: organización, procesos y procedimientos, rutinas de gestión, personal, ambiente físico, configuración del sistema de información, hardware, software y equipo de comunicaciones.

d) ***Salida:*** listado de vulnerabilidades y su relación con los activos, amenazas y controles.

Identificación de Consecuencias

a) ***Entrada:*** listado de activos, procesos del negocio, amenazas y vulnerabilidades.

b) ***Acción:*** identificación de las consecuencias como resultado de pérdidas de confidencialidad, integridad y disponibilidad de los activos.

c) ***Guía para la implementación***: Los incidentes producen consecuencias o daños en uno o varios activos. Un incidente describe una amenaza que explota una o varias vulnerabilidades. El impacto se determina al establecer el contexto y el valor del activo en base al grado de afectación que haya tenido la empresa ya sea de forma temporal o permanente. Las consecuencias pueden ser ocasionadas por pérdida de tiempo de investigación y reparación del activo, pérdida de oportunidad y de tiempo, salud y seguridad, el costo financiero, imagen, reputación y buen nombre.

d) ***Salida:*** listado de posibles incidentes, consecuencias, activos y procesos del negocio que pueden verse afectados.

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.

Valoración de Consecuencias

a) *Entrada:* listado de los incidentes, amenazas, vulnerabilidades, activos y procesos del negocio afectados.

b) *Acción:* evaluación del impacto de los incidentes y análisis de las consecuencias.

c) *Guías para la implementación*: el valor del impacto en el negocio se puede expresar de manera cualitativa y cuantitativa; sin embargo asignar un valor monetario a los activos facilita la toma de decisiones. La extrapolación de los datos obtenidos como resultado de eventos ocurridos permite medir las consecuencias.

d) *Salida**:*** listado activos, criterios de impacto y consecuencias de un incidente.

Valoración de Incidentes

a) *Entrada:* listado de incidentes, amenazas, activos afectados, vulnerabilidades explotadas, consecuencias a nivel de activos, procesos del negocio y controles existentes y planificados.

b) *Acción**:*** evaluar la probabilidad de ocurrencia de los incidentes

c) *Guías para la implementación*: evaluar la probabilidad y el impacto de que ocurra un incidente utilizando técnicas de estimación cualitativas y cuantitativas. Analizar la frecuencia, la probabilidad de ocurrencia de las amenazas accidentales o deliberadas y la vulnerabilidad de los activos y la eficacia de los controles.

d) *Salida**:*** probabilidad de ocurrencia de un incidente evaluada.

Nivel de Estimación de Riesgos

a) *Entrada**:*** incidentes, consecuencias, activos y procesos de negocios, probabilidad de ocurrencia.

b) *Acción*: estimación del nivel de riesgo.

c) *Guía para la implementación*: evaluar las consecuencias de un riesgo, la probabilidad de ocurrencia de un incidente; y asignarles valores cualitativos o cuantitativos.

d) *Salida**:*** listado de riesgos estimados.

Evaluación de Riesgos

a) *Entrada*: listado de riesgos, niveles de valor asignados y criterios de evaluación del riesgo.

b) *Acción**:*** comparar los niveles de riesgo frente a los criterios de evaluación y aceptación del riesgo, definidos en el establecimiento del contexto.

c) *Guía para la implementación*: comparar los riesgos estimados y los criterios que se evaluaron para la toma de decisiones, con el contexto definido para gestionar el riesgo, sin perder de vista los objetivos de la organización; y realizar un análisis del riesgo que permita tomar decisiones, garantizando un nivel de riesgo aceptable. Los riesgos globales deben considerar la criticidad de los procesos del negocio.

d) Salida: listado de riesgos, prioridades, criterios de evaluación e incidentes que puedan ocasionarlos.

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. La estructura de la actividad es la siguiente:

a) *Entrada*: riesgos, prioridades, incidentes y criterios de evaluación del riesgo.

b) *Acción:* seleccionar controles para reducir, retener, evitar y transferir los riesgos y elaborar un plan para el tratamiento del riesgo.

c) *Guía para la implementación*: las opciones para el tratamiento del riesgo: reducir, retener, evitar y transferir el riesgo.

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.

Reducción del Riesgo

a) *Acción:* Reducir el nivel del riesgo mediante la selección de controles hasta obtener un riesgo residual aceptable.

b) *Guía para la implementación:*

a. Disminuir costo total de propiedad del sistema a través de controles que incluyan criterios de aceptación del riesgo, costos, tiempo de implementación, aspectos técnicos, ambientales y culturales
b. Definir costos de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles; y compararlos con el valor del activo que se protege
c. Analizar el retorno de la inversión en términos de reducción del riesgo
d. Analizar las restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, de personal, de integración de controles nuevos y existentes y su facilidad de uso

e. Identificar una solución que garantice la seguridad de la información y asegurar que las restricciones de carácter técnico implementadas a través de un control, no afecten su desempeño.

c) *Salida**:*** Controles posibles, costos, beneficios y prioridades de implementación.

Retención del Riesgo

a) *Acción*: evaluar si se debe mantener el riesgo.

b) *Guía para la implementación*: Analizar si los criterios utilizados para aceptar y retener son suficientes o si es necesario implementar controles adicionales.

Evitar el Riesgo

a) *Acción*: evitar la acción que da origen al riesgo particular.

b) *Guía para la implementación*: analizar el impacto del riesgo y el costo de implementar el tratamiento versus el beneficio a obtener; y decidir si se evita el riesgo modificando las actividades y las condiciones bajo las cuales se efectúan.

Transferir el Riesgo

a) *Acción**:*** transferir el riesgo en base a su evaluación.

b) *Guía para la implementación*: al transferir un riesgo podemos crear nuevos o modificar los actuales, lo que implica repetir el tratamiento. Para evitar que el sistema de información sufra ataques, se lo monitorea de forma constante. La gestión del riesgo puede ser transferida a un tercero sin embargo, la organización es responsable del impacto en caso de que este ocurra.

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.

Aceptación del riesgo

a) *Entrada:* plan de tratamiento del riesgo y valoración del riesgo residual.

b) *Acción:* aceptar los riesgos y definir y registrar responsabilidades.

c) *Guía para la implementación*:

   a. Definir la forma de tratar el riesgo valorado en el plan de tratamiento, considerando los criterios de aceptación establecidos
   b. Analizar y aprobar el plan de tratamiento del riesgo, los riesgos residuales y las condiciones de aceptación establecidas para su aprobación
   c. Analizar si el riesgo residual cumple los criterios de aceptación del riesgo y si circunstancias preponderantes fueron consideradas. Si no se lo hizo, hay que justificarlo indicando el alto costo de reducir el riesgo y el beneficio a ser obtenido
   d. Revisar oportunamente los criterios de aceptación del riesgo previo a su aceptación y justificación.

d) *Salida:* Riesgos aceptados y justificados.

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.

Factores de Riesgo

a) *Entrada*: Actividades de gestión del riesgo

b) *Acción:* Analizar de forma oportuna y continua el contexto y los cambios producidos en los factores de riesgos para mantener controlado el riesgo. Los factores de riesgo son el valor de los activos, las amenazas, los incidentes y la probabilidad de ocurrencia, para mantener controlado el riesgo.

c) *Guía para la implementación*: Si se detecta cambios en el valor de los activos existentes o recién adquiridos, que pueden ser vulnerables a amenazas y cuya probabilidad de ocurrencia sea alta, se debe revisar si las opciones seleccionadas para tratar el riesgo son adecuadas. Para identificar que el riesgo tenga un nivel aceptable, se debe adoptar medidas de control como agrupar los riesgos bajos y que han sido aceptados, y evaluar su impacto potencial acumulado.

d) *Salida**:*** relacionar de forma continua los objetivos del negocio con los objetivos de la gestión del riesgo y los criterios de aceptación.

Gestión del Riesgo

a) *Entrada**:*** Actividades de gestión del riesgo.

b) *Acción:* Chequear de forma sistemática el proceso de gestión del riesgo.

c) Guía para la implementación:

a. Revisar los resultados de valorar y tratar el riesgo, validar la vigencia de la gestión del riesgo y la continuidad de los planes de gestión
b. Informar a las autoridades y a los interesados de las mejoras del proceso de gestión del riesgo

c. Analizar los criterios de impacto, evaluación y aceptación del riesgo, que deben estar acordes a las estrategias del negocio, y a los cambios legales, ambientales y de mercado
d. Disponer de recursos económicos para realizar el monitoreo de la gestión del riesgo
e. Detectar cambios que modifiquen el objeto del proceso de la gestión del riesgo

d) *Salida:* Adaptar continuamente el proceso de la gestión riesgo de la seguridad de información a los objetivos del negocio.

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.

Anexos

Atributos de la gestión mejorada del riesgo

El alto nivel de desempeño de una organización en la gestión del riesgo es posible medirlo mediante el uso indicadores, que comparan los criterios considerados como atributos. Entre los atributos que mencionaremos a continuación tenemos los siguientes:

a) Mejora continua
b) Rendición total de cuentas con respecto a los riesgos
c) Aplicación de la gestión del tiempo en la toma de decisiones
d) Comunicaciones Continuas
e) Integración completa en la estructura del gobierno.

Mejora Continua

Los indicadores que miden el desempeño de la gestión del riesgo a través de la mejora continua son:

- Establecer metas de desempeño de la organización a nivel de procesos, sistemas, recursos, capacidad y habilidades
- Medir el desempeño de la organización, del director individual, de los departamentos e individuos
- Revisión anual de desempeño de la organización previo a establecer objetivos del próximo período
- Valoración del desempeño de la gestión del riesgo
- Comunicar y publicar anualmente el desempeño de la organización.

Rendición Total de Cuentas con respecto a los riesgos

La gestión mejorada del riesgo incluye la rendición de cuentas exhaustiva, completamente definida y aceptada de los riesgos, los controles y las tareas para el tratamiento y monitoreo de los riesgos, a cargo del personal responsable del proceso y que constituyen el indicador que medirá la gestión; la misma que deberá ser comunicada oportunamente a las partes internas y externas de la organización.

Aplicación de la Gestión del tiempo en la toma de decisiones

La toma de decisiones involucra la gestión expresa de los riesgos y la aplicación de la gestión del riesgo. El indicador es el registro de las reuniones, donde se tomaron decisiones claras sobre los riesgos y sus componentes, relacionadas a los proyectos críticos e importantes para la organización.

Comunicaciones Continuas

Comunicar el desempeño de la gestión del riesgo a las partes involucradas externas e internas de la organización constituye el indicador que mide este atributo de la gestión del riesgo. Una comunicación

constante sobre el desempeño de la gestión del riesgo, ayuda a que la toma de decisiones sea la apropiada.

Integración completa en la estructura del Gobierno

Para lograr los objetivos de una organización es importante gestionar el riesgo de forma eficiente. El lenguaje utilizado por los directores de una organización puede ser considerado el indicador, para medir la integración que existe con el proceso de los riesgos, a más de la documentación existente en las políticas de la organización.

Definición del alcance y los límites del proceso de la gestión del riesgo en la seguridad de la información

Definir la identidad de una organización implica determinar su misión, valores, principios, objetivos, estrategias y su estructura interna. Conocer la estructura interna es identificar como funciona cada una de las áreas, y los servicios y productos que vende a sus clientes. Una organización puede estar estructurada por áreas y/o funcionalmente, y esto se representa gráficamente en el cuadro de la organización e incluye las autoridades, las líneas de reporte, y las relaciones y flujos de información existentes. La estrategia organizacional muestra el camino a seguir para lograr la rentabilidad deseada.

Restricciones que afectan a la Organización

Para determinar cuál es la dirección que se debe tomar en relación a la seguridad de la información se deben considerar las restricciones internas y/o externas que existen. Identificar las brechas existentes en la seguridad de la información puede significar volver a definir los objetivos estratégicos de la organización. El sistema de información facilita la implementación de la seguridad de la información.

Las restricciones que existen pueden ser: de naturaleza política, estratégica, territoriales, estructurales, funcionales, de personal, organizacionales, culturales, y presupuestaria. A más de técnicas, relacionadas con la infraestructura de hardware y software y comunicaciones, edificaciones, ambientales, organizacionales, tiempo de implementación de controles de seguridad.

Identificación y valoración de los activos e impactos

Para valorar los activos, previamente deben ser identificados. Los activos son de dos tipos, primarios y de soporte.

Los activos primarios son la información, las actividades y los procesos del negocio. Los activos de soporte son de hardware, software, redes, personal, ubicación y estructura de la organización. Para identificar los activos primarios se requiere formar usuarios.

Los procesos de la organización considerados como activos primarios, deben seguir una política de seguridad de información y/o un plan de continuidad del negocio, que eviten que su pérdida afecte el cumplimiento de la misión, los aspectos legales y las estrategias de la organización. La información primaria es aquella considerada como sensible, privada, estratégica, y de alto costo, y crítica para el logro de los objetivos. Los límites del alcance del estudio lo define la criticidad del mismo.

Los activos de soporte son aquellos cuyas vulnerabilidades son afectados por las amenazas cuya intención es dañar los activos primarios. Pueden ser de diferentes tipos, entre los que podemos mencionar están los de: hardware, software, sistema operativo, software de servicio, paquetes de software, aplicaciones del negocio, redes y comunicaciones, personal, instalaciones físicas, servicios, y la estructura organizacional.

Valoración de Activos

La organización debe determinar si realiza una valoración cuantitativa o cualitativa de los activos y depende del tipo de activos que se analiza. Los términos que se utilicen en una valoración cualitativa, pueden ser: insignificante, muy bajo, bajo, medio, alto, muy alto y crítico.

Los criterios para estimar el valor de un activo, son su costo original, el costo de reposición, y el costo por la pérdida de integridad o disponibilidad debido a incidentes de seguridad, por lo que identificar el impacto es indispensable, para valorar el daño de un activo. En ciertos casos un activo puede tener varios valores durante el proceso de valoración, por lo que es necesario que se defina la forma en que va a asignar el mismo, podría ser la sumatoria de varios valores, o el valor máximo estimado.

Para evaluar el impacto por pérdida de confidencialidad, integridad, disponibilidad, y confiabilidad, se utiliza criterios como las consecuencias financieras, afectación de la imagen y reputación de la compañía, incumplimientos legales, problemas de operación y contractuales, seguridad de empleados y usuarios, entre otros.

La organización debe establecer una escala para valorar a los activos, que pueden ser alto, medio o bajo, o niveles entre 3 y 10. Sin embargo para estimar pérdidas financieras, los valores monetarios son los apropiados. Un activo mantiene su valor, si los activos dependientes de él, tienen un valor menor o igual, caso contrario, su valor debe incrementarse; para lo cual debe determinarse el nivel de dependencias y los valores de los activos dependientes. El resultado de la valoración de los activos, es un listado que incluye los activos y la valoración realizada.

Valoración de Impactos

Los incidentes pueden generar consecuencias inmediatas o futuras en los activos. El impacto inmediato puede ser directo o indirecto.

A nivel operacional se ve afectada de forma directa la seguridad de la información, el costo de adquisición o reposición de los activos, el costo operacional por falta de servicio, y el valor financiero de reposición. El impacto indirecto se considera el costo de oportunidad, los costos de operación y el posible mal uso de la información ocasionado por fallas de seguridad.

Tipos de Amenazas

Las amenazas pueden ser deliberadas, accidentales o ambientales. Las acciones deliberadas, se enfocan a los activos de la organización, las accidentales son aquellas que de forma accidental pueden dañar los activos, y las ambientales o naturales, son aquellas no realizadas por las personas. Las amenazas pueden ser de los siguientes tipos:

- Daño físico
- Eventos naturales
- Pérdida de servicios esenciales
- Perturbación debido a la radiación
- Compromiso de la información
- Fallas técnicas
- Acciones no autorizadas
- Compromiso de las funciones

Las fuentes de las amenazas humanas se consideran a los intrusos, piratas, criminales, terroristas y al espionaje industrial entre otras.

Métodos de Valoración de Vulnerabilidades

Las vulnerabilidades en áreas de seguridad de la información puede ser de: hardware, software, red, personal, lugar o ubicación, y organización.

Para valorar las vulnerabilidades técnicas, se pueden utilizar métodos de prueba, tales como: herramientas automáticas para explorar vulnerabilidades, pruebas de análisis de código para evaluar la vulnerabilidad del sistema, pruebas de penetración y evaluación de la capacidad y seguridad de los sistemas de información y comunicación.

Valoración de riesgos en la seguridad de la información

La valoración de alto nivel determina qué acciones son prioritarias y cuando deben ser ejecutadas. Se inicia con una valoración de alto nivel de las consecuencias, y una sincronización con los planes de gestión de cambios. La valoración de riesgos permite:

1. Analizar el contexto orientado al negocio y su operación, y no en los componentes tecnológicos
2. Agrupar en dominios una lista de amenazas y vulnerabilidades y definir escenarios de posibles ataques
3. Seleccionar listas de controles para cada dominio que serán validadas a través de todo el sistema
4. Proveer y gestionar controles organizacionales y salvaguardas técnicas críticas y comunes.

Además facilita la aceptación del programa de valoración de riesgos, y la definición de la estrategia de un programa de seguridad de información que proteja a los sistemas más vulnerables.

Los factores que indican si la valoración de riesgos de alto nivel es adecuada para para tratar los riesgos son:

- Los objetivos del negocio a ser alcanzados
- El nivel de dependencia del negocio respecto a los activos de información
- La inversión realizada para cada activo

- Los activos de información a los cuales se asignó un valor

El proceso valoración detallada de los riesgos se utiliza para sistemas de información en alto riesgo y se inicia con la identificación y valoración profunda de activos, amenazas y vulnerabilidades y luego se continúa con la evaluación y tratamiento del riesgo.

Evaluar las consecuencias es posible mediante el uso de medidas cuantitativas y/o cualitativas. Si se requiere analizar la probabilidad de que ocurra una amenaza, se debe considerar cual sería el impacto ante una amenaza humana deliberada, el beneficio que se logra si el activo es vulnerado y que tan vulnerable es de ser explotado.

Métodos de Valoración de Riesgos

1. Matriz con valores predefinidos

Los activos físicos y el software real o propuesto, se cuantifica a nivel de costos de reemplazo, reconstrucción o compra. Estos valores se transforman en escalas cualitativas.

Para valorar la información, su probabilidad de ocurrencia y las consecuencias, se entrevistan a los dueños de los datos que conocen el grado de afectación del negocio, en caso de no disponer de la misma. Se usa además escalas cuantitativas y/o cualitativas en el análisis de temas legales y reglamentos, pérdidas financieras, operaciones, seguridad, imagen corporativa, entre otros.

Los cuestionarios se utilizan para valorar la probabilidad de ocurrencia de una amenaza y la vulnerabilidad de un activo ante una amenaza. Al elaborar los cuestionarios se deben agrupar los activos por tipo de amenaza y de consecuencias. A las respuestas obtenidas se les asignan diferentes puntajes.

A continuación se detalla en una matriz, el valor del activo, la probabilidad de ocurrencia de una amenaza, la vulnerabilidad del activo, y el nivel del riesgo cuyo rango fluctúa entre 1 y 8 para el ejemplo.

Tabla 13

Nivel de Riesgo

	Amenaza Probabilidad de ocurrencia	**Baja**			**Media**			**Alta**		
	Vulnerabilidad Facilidad de Explotación	b	M	a	b	m	a	b	m	a
Valor del activo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Valor del activo: 0 – 4

Probabilidad de Ocurrencia Amenaza: baja, media y alta

Facilidad de Explotación de una vulnerabilidad: baja, media y alta

Ejemplo: Valor del activo = 3, Amenaza = alta, vulnerabilidad = baja

Nivel de riesgo = 5

En la siguiente tabla se analiza la probabilidad de que un incidente ocurra, su impacto en el negocio y el valor del riesgo resultante en un rango de 1 a 8 para el ejemplo:

Tabla 14

Probabilidad de Ocurrencia de un Incidente

	Probabilidad del escenario del incidente	**Muy baja (muy improbable)**	**Baja (improbable)**	**Media (posible)**	**Alta (probable)**	**Muy alta (frecuente)**
Impacto en el negocio	Muy baja	0	1	2	3	4
	Baja	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Muy Alta	4	5	6	7	8

Riego bajo: 0-2, Riesgo medio: 3-5, Riesgo alto: 6-8

2. Clasificación de las amenazas y su nivel de riesgo

A continuación se detalla en la tabla los activos, las consecuencias, la probabilidad de ocurrencia de una amenaza y el nivel del riesgo si ocurre el incidente.

Tabla 15

Clasificación de Amenazas

Amenaza	Consecuencia	Probabilidad de ocurrencia de la Amenaza	Medida de riesgo	Clasificación de la amenaza
A1	1	5	5	3
A2	2	4	8	2
A3	3	3	9	1
A4	4	2	8	4
A5	2	1	2	3
A6	5	3	15	5

Valor del activo: 1 - 5

Probabilidad de Ocurrencia Amenaza: 1 - 5

Valor del Riesgo: Consecuencia * Probabilidad de Ocurrencia de la amenaza

Clasificación de la amenaza: 1 – 5; 1, valor más bajo y 5 el más alto.

3. Probabilidad de ocurrencia de una amenaza y sus consecuencias

En caso de ocurrir una amenaza que afecte a los activos que son parte de un sistema, es necesario realizar una evaluación de los activos, las amenazas y su probabilidad de ocurrencia y las consecuencias o impacto, si el activo es amenazado. Los pasos a seguir serían los siguientes:

1. Se evalúan los activos y los riesgos
2. Se suman los valores de los activos y se define una medida de riesgo del sistema
3. Se asigna un valor a cada activo y se lo asocia a las consecuencias de las amenazas.
4. Se suman al activo amenazado los valores de las amenazas
5. Se evalúa el valor de la probabilidad, y se obtiene la probabilidad de ocurrencia y el valor de la vulnerabilidad (*Tabla 17)*

6. Se asigna un puntaje activo/amenaza determinado en la intersección del activo y de la probabilidad en la tabla 18
7. Se obtiene el valor total de activo a través de una sumatoria de los valores activo/amenaza
8. Se totalizan los activos y se obtiene el valor del Sistema.

Tabla 16

Probabilidad de un incidente

Probabilidad de amenaza	Baja			Media			Alta		
Vulnerabilidad	B	M	A	B	M	A	B	M	A
Probabilidad de incidente	0	1	2	1	2	3	2	3	4

Tabla 17

Valor activo y probabilidad

Valor del Activo	0	1	2	3	4
Valor de la Probabilidad					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

9. A continuación se realiza un ejemplo del proceso antes indicado:
   a. El sistema S tiene 3 activos: A1, A2 y A3 y 2 amenazas T1 y T2
   b. El valor de A1 es 3, A2 es 2, A3 es 4
   c. Si para A1/T1: la probabilidad de la amenaza es baja y la facilidad de la explotación de la vulnerabilidad es media. Resultado, Probabilidad = 1 (*Figura No. 17)*
   d. El puntaje del activo/amenaza A1/T1 se obtiene de la tabla e4.
   A1 = 3, T1 = 1; A1+T1=4
   e. De igual modo A1/T2, la probabilidad de la amenaza es media y la facilidad de explotación de la vulnerabilidad es alta, A1/T2 es 6
   f. Puntaje total A1 = A1/T1 + A1/T2 = 4 + 6 = 10
   g. TS = Total del sistema = A1T + A2T + A3T.

Restricciones para la reducción del riesgo

Las restricciones para reducir los riesgos que se deben considerar son de tipo financiera, técnica, operativa, cultural, ética, ambiental, legal, facilidad de uso, de personal y de integración de controles nuevos y existentes.

Las restricciones relacionadas al tiempo, son aquellas relacionadas a la implementación de los controles durante el tiempo de vida de una aplicación, y su exposición al riesgo.

Las restricciones financieras, se refieren al costo de implementar los controles, el mismo que no debe superar el valor del riesgo a ser evitado. En ciertos casos cuando se valor presupuestado puede ser excedido, corresponde a las autoridades tomar la decisión de hacerlo o no.

Las restricciones técnicas, se deben a fallas en la implementación de los controles debido a dificultades técnicas u operativas, o al no logro en la reducción de los riesgos. En estos casos es conveniente revisar el funcionamiento del sistema de seguridad de la información.

Las restricciones operativas, que generen costos altos en la implementación de los controles deben ser analizados por la organización.

Las restricciones de tipo cultural y ético que pueden existir en una sociedad, dificultan la implementación de los controles y a su aceptación por parte del personal de la organización.

Las restricciones ambientales, tales como la geografía, el clima, las catástrofes, etc., determinan el nivel de controles que pueden ser implementados.

Entre las restricciones legales, que afectan la selección, implementación y uso de controles están las leyes y reglamentos existentes a nivel, financiero, regulatorio, laboral, entre otras.

La facilidad de utilización de los controles, que tienen un nivel de riesgo residual tolerable, determina su nivel de aceptación dentro del negocio. La contratación del personal capacitado, con experiencia y que esté disponible cuando se requiere puede dificultar la implementación de los controles. El personal especializado, implica salarios altos, que deben ser considerados por la organización. Es conveniente analizar la integración de los nuevos controles con la infraestructura existente y los controles ya existentes, ya que en ocasiones la misma no es posible, o implica costos altos para el negocio.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Este estudio se enfocó en el análisis de las similitudes y diferencias de las normas ISO/IEC 31000 e ISO/IEC 27005 con la finalidad de determinar la factibilidad de su integración y complementariedad. Lo cual se confirmó a través de mapeos de alto nivel y mapeos detallados de secciones específicas, que incluyeron sus estructuras, procesos, conceptos y anexos.
- La diferencia básica encontrada entre ambas normas, es que la ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que la ISO/IEC 27005 lo hace de forma específica en la Gestión de Riesgos en la Seguridad de la Información. Sin embargo existe similitud en muchos de los procesos y en la terminología utilizada al definir sus conceptos.
- Mientras que la ISO/IEC 31000 detalla a nivel de anexos los atributos que debe tener la gestión del riesgo, a manera informativa la ISO/IEC 27005 se enfoca en identificar los activos e impactos, las amenazas a las que están expuestos, el análisis de las vulnerabilidades, y el análisis de riesgos de forma específica y muy concreta, y es aquí donde se encuentran las mayores diferencias, por el enfoque que realiza la norma.
- Al examinar las normas ISO/IEC 31000 e ISO/IEC 27005 se detecta que sus fundamentos organizacionales y la forma de planificar y ejecutar los proyectos son parecidas.
- La consistencia de análisis realizado se prueba con el desarrollo del modelo integrado sobre la base de las normas ISO/IEC 31000 e ISO/IEC 27005.

5.2 Recomendaciones

- Utilizar marcos de trabajo y metodologías de análisis y gestión del riesgo que apoyen la integración de las normas ISO/IEC 31000 e ISO/IEC 27005 orientadas a la Gestión del Riesgo con otras consideraciones como por ejemplo COBIT como marco de referencia para el Gobierno de TI, ITIL para gestión de servicios de TI
- Utilizar el resultado de la integración realizada en casos prácticos relacionados con la gestión de riesgos en la seguridad de la información o con la gestión de riesgos en general
- Estudiar la forma de generalizar los procesos de comparación, integración y complementariedad de normas y estándares a partir de la experiencia obtenida de este trabajo.

BIBLIOGRAFÍA

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/

CARTA DE AUSPICIO

Por medio del presente, yo Ing. Carlos Montenegro en mi calidad de profesor del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, certifico el auspicio a la tesis: "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", a ser desarrollada por las Srta. Myrian Alexandra Medina Tapia; para lo cual le proporcionaré la información requerida para la elaboración del proyecto de titulación en mención.

Sangolquí, 6 de Enero de 2015

Ing. Carlos Montenegro
PROFESOR
CIENCIAS DE LA COMPUTACIÓN

CARTA DE ACEPTACIÓN

Por medio del presente, yo Ing. Carlos Montenegro en mi calidad de profesor del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, certifico que la Srta. Myrian Alexandra Medina Tapia ha culminado el desarrollo de la tesis titulada: "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", por lo cual se acepta el proyecto de titulación en mención.

Sangolquí, 19 de Junio de 2015

Ing. Carlos Montenegro
PROFESOR
CIENCIAS DE LA COMPUTACIÓN

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

_____

Myrian Alexandra Medina Tapia

_____

Ing. Mauricio Campaña

DIRECTOR DE CARRERA

Sangolquí, Julio de 2015

HOJA DE VIDA

INFORMACIÓN GENERAL

Nombre: Myrian Alexandra Medina Tapia
C.I. 1303252421
Email: miriam.medina.tapia@gmail.com
Celular: 099 5653936

EDUCACIÓN

Facultad Latinoamericana de Ciencias Sociales, FLACSO, Quito
Maestría en Economía y Gestión Empresarial Pymes, 2011-2013 (egresada)

Tecnológico de Monterrey, Quito
Diplomado en Habilidades Gerenciales, 2007

Universidad San Francisco de Quito, Quito
Diplomado Especialización Gerencial en Gerencia y Marketing, Finanzas y Proyectos, 2001

Escuela Politécnica del Ejército, Quito
Ingeniería de Sistemas e Informática, 1996 (egresada)
Tecnología y Análisis de Sistemas, 1990

IDIOMAS

Inglés - *Wooster High School y College of Wooster, Wooster, Ohio, USA, 1983*
Francés - *Alianza Francesa de Quito, Ecuador 2008 – 2009*
Alianza Francesa de Rouen, Francia 2009

DESCRIPCIÓN DE CARRERA

Municipio del Distrito Metropolitano de Quito, MDMQ
Jefe de Redes y Comunicaciones, Mayo 2014 – Enero 2015

Agencia Nacional de Tránsito, Transporte y Seguridad Vial, ANT
Directora Tecnología Informática, Diciembre 2011 – Agosto 2012
Asesora Tecnologías de la Información, Agosto 2012 – Diciembre 2012

Ministerio Coordinador de la Producción, Empleo y Competitividad, MCPEC
Consultora de Proyectos de Tecnología Informática, Agosto 2010 – Octubre 2011
Asesora de Tecnología Informática, Noviembre 2009 - Julio 2010

Ministerio Coordinador de Desarrollo Social, MCDS
Directora de Gestión Tecnológica, Febrero 2008 – Noviembre 2009

Telefónica – Movistar
Team Leader Testing – Quality Asssurance, Octubre 2006 - Octubre 2007

Xerox del Ecuador
Client Services Manager, Xerox Global Services, Octubre 2005 - Julio 2006

Maint
Gerente de Producto – Software y Educación, Julio 2004 - Septiembre 2005
Coordinadora de Servicios Profesionales, Mayo 2001 - Junio 2004

Ecuador Bootling Company (Embotellador de Coca Cola)
Jefe de Sistemas de Gaseosas del Tungurahua, GATSA, Octubre 1994 - Noviembre 1999

Automotores y Anexos, NISSAN
Jefe de Sistemas, 1991 - Octubre 1994

Terncap
Analista de Sistemas, 1989 - 1990

Banco Continental
Oficial de Mercadeo y Cajera, 1985 – 1989

ACTIVIDADES Y LOGROS EXTRACURRICULARES

- Universidad San Francisco de Quito - *Profesor del Politécnico: Administración de Centros de Cómputo, Auditoría de sistemas y Modelos de Decisión; 2003 – 2004*
- Club Rotario Quito Metropolitano, *socia activa desde su fundación en el año 2002 hasta el año 2005*

SEMINARIOS Y TALLERES

Habilidades Gerenciales INCAE (Managua 1997); Computer Associates World (Orlando 2002); Itil Foundations, Santa Mónica Consulting (2005); Six Sigma XEROX (2006); Introducción al PMBook Gerencia de Proyectos basada en Gerencia del Procesos y Preparación Certificación Project Management Professional PMI (Marwep Consulting Group, Noguera 2008 y 2010), Programa Actualización de conocimientos, ESPE (2013-2014)