Escuela Superior de Redes RED CEDIA

GESTIÓN DEL RIESGO DE LAS TI NTC 27005

VERSIÓN ORIGINAL:
Edson Kowask Bezerra
Fabiano Alcántara Lima
Alexandre Cesar Motta
Jacomo Dimmit Boca Piccolini

VERSIÓN ADAPTADA AL ECUADOR
A partir de la versión de
ESR RENATA -Colombia

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Gestión del riesgo de las TI NTC 27005

Versión original:
Edson Kowask Bezerra
Fabiano Alcántara Lima
Alexandre Cesar Motta
Jacomo Dimmit Boca Piccolini

Versión adaptada al Ecuador
A partir de la versión de
ESR RENATA - Colombiav

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Escuela Superior de Redes RED CEDIA

Red Nacional de Tecnología Avanzada - RENATA

Director Ejecutivo
Lucas Giraldo Rios

Gerente de Comunicaciones
Camilo Jaimes Ocazionez

Gerente Administrativo y Financiero
Jader Alexis Castaño

Gerente de Tecnología e Información
Javier Enrique Lizarazo Rueda

Escola Superior de Redes - RNP Brasil

Título original "Gestão da Riscos de TI NBR 27005"
Versión portuguesa RNP ©

Autores versión portuguesa
Flavia Estélia Silva Coelho
Luis Geraldo Segadas de Araújo
Edson Kowask Bezerra

Universidad Nacional de Colombia Facultad de Ingeniería

Decano
José Ismael Peña Reyes

Vicedecano Académico
Oscar Germán Duarte

Director Instituto de Extensión e Investigación
Carlos Cortés

Coordinadora Académica
Jenny Marcela Sánchez-Torres

Autora versión adapatada y ampliada
Ingrid Patricia Páez Parra

Traductor
Oscar Edwin Piamba Tulcán

Profesionales de apoyo
Ana Carolina Gómez Parra

Diseño y diagramación
Andrés Camilo Gantiva Rueda

ISBN: (ebook)

Comentarios y preguntas (versión ESR - Colombia)

Envíe sus comentarios y preguntas sobre esta publicación a:
RENATA - Escuela Superior de Redes – ESR Colombia.
E-mail: esrcolombia@renata.edu.co
www.renata.edu.co
Bogotá D.C. - Colombia

Prólogo a la versión portuguesa

La Escuela Superior de Redes, ESR, es una unidad de la Rede Nacional de Ensino e Pesquisa, RNP, responsable por la difusión del conocimiento en Tecnologías de la Información y Comunicación, TIC. La ESR nace con la propuesta de ser formadora y diseminadora de las competencias en TIC para el cuerpo técnico – administrativo de las universidades federales, escuelas técnicas y unidades federales de investigación. Su misión fundamental es realizar la capacitación técnica del cuerpo funcional de las organizaciones usuarias de la RNP, para el ejercicio de las competencias aplicables al uso eficaz y eficiente de las TIC.

La ESR ofrece decenas de cursos en áreas temáticas como: administración y proyecto de redes, administración de sistemas, seguridad, medios de soporte a la colaboración digital de gobierno de TI.

La ESR también participa en diversos proyectos de interés público, como la elaboración y ejecución de planes de capacitación para la formación de multiplicadores para proyectos educativos como: formación en el uso de video conferencia para la Universidad Abierta de Brasil, UAB, formación de soporte técnico de laboratorios del Proinfo y creación de un conjunto de cartillas sobre redes inalámbricas para el programa Un Computador por Alumno, UCA.

Prólogo a la versión en castellano

La Red Nacional Académica de Tecnología Avanzada, RENATA, tiene el gusto de presentarle a la comunidad académica, científica, tecnológica y empresarial del país, la Escuela Superior de Redes (ESR) RENATA Colombia, esfuerzo de colaboración con la Rede Nacional de Ensino y Pesquisa, RNP Brasil e Instituciones de Educación Superior en Colombia, como parte de nuestra estrategia STAR (Servicios de Tecnología Avanzada RENATA).

Nuestro objetivo es la formación de alto nivel en competencias TIC para todo el personal técnico, administrativo y académico del país, tanto de instituciones conectadas como no conectadas a RENATA de modo tal que se permita incrementar y mejorar la eficiencia en el uso de las tecnologías de la información y las comunicaciones para el trabajo colaborativo en Colombia.

Es también este el espacio para agradecerle a RNP y las universidades del país que han participado en la construcción de este programa académico, junto con los profesores y técnicos que pusieron todo de sí para llevar a buen puerto esta iniciativa.

RENATA los invita a todos a sacarle el mayor provecho a este proceso formativo y a beneficiarse de todo el potencial y los Servicios de Tecnología Avanzada RENATA, STAR.

RENATA es la red nacional de investigación y educación de Colombia que conecta, articula e integra a los actores del Sistema Nacional de Ciencia Tecnología e Innovación (SNCTI) entre sí y con el mundo, a través del suministro de servicios, herramientas e infraestructura tecnológica para contribuir al mejoramiento del nivel de productividad, efectividad y competitividad de la producción científica y académica del país.

Metodología de la ESR

La filosofía pedagógica y la metodología que orientan los cursos de la ESR están basadas en el aprendizaje como construcción del conocimiento por medio de la resolución de problemas típicos de la realidad del profesional en formación. Los resultados obtenidos en los cursos de naturaleza teórico-práctica son optimizados, pues el instructor, ayudado por el material didáctico, actúa no solo como un expositor de conceptos e información, pero si principalmente como orientador del alumno en la ejecución de las actividades contextualizadas en las situaciones de su cotidiano profesional.

El aprendizaje es entendido como una respuesta del alumno al desafío de situaciones-problemas semejantes a las encontradas en la práctica profesional, que son superadas por medio del análisis, síntesis, juzgamiento, pensamiento crítico y construcción de hipótesis para la solución del problema, en abordajes orientadas al desarrollo de competencias.

Así, el instructor tiene participación activa y dialogada como orientador del alumno para las actividades en el laboratorio. Inclusive la presentación de la teoría al inicio de la sesión de aprendizaje no es considerada una simple exposición de conceptos e información. El instructor busca incentivar la participación de los alumnos continuamente.

Las sesiones de aprendizaje en las que se realiza la presentación de contenidos y la realización de las actividades prácticas tienen formato presencial y esencialmente práctico, utilizando técnicas de estudio dirigido individual, trabajo en equipo y prácticas orientadas al contexto de actuación del futuro especialista que se pretende formar.

Las sesiones de aprendizaje se desarrollan en tres etapas, con mayor dedicación a las actividades prácticas, conforme a la siguiente descripción:

Primera etapa: presentación de la teoría y solución de dudas (de 60 a 90 minutos)

El instructor presenta, de manera sintética, los conceptos teóricos correspondientes al tema de la sesión de aprendizaje, con ayuda de diapositivas en formato Power Point. El instructor formula interrogantes sobre el contenido de las diapositivas en lugar de solo presentarlas, animando al grupo a la participación y la reflexión. Eso evita que las presentaciones sean monótonas y que el alumno tenga una actitud pasiva, lo que reduciría el aprendizaje.

Segunda etapa: actividades prácticas de aprendizaje (de 120 a 150 minutos)
Esta etapa es la esencia de los cursos de la ESR. La mayoría de las actividades de los cursos es asincrónica y realizada en grupos de dos alumnos, que siguen el ritmo de la guía de actividades propuesta en el libro de apoyo. El instructor y el monitor circulan entre los grupos para solucionar las dudas y ofrecer explicaciones complementarias.

Tercera etapa: discusión de las actividades realizadas (30 minutos)
El instructor comenta cada actividad, presentando una de las soluciones posibles, prefiriendo aquellas que generan mayor dificultad y polémica. Los alumnos son invitados a comentar las soluciones encontradas y el instructor retoma tópicos que hayan generado dudas, estimulando la participación de los alumnos. El instructor siempre estimula a los alumnos a encontrar soluciones alternativas a las sugeridas por él y por sus colegas, en caso que existan, y a comentarlas.

Sobre el curso

El objetivo del curso es introducir los principios básicos de gestión del riesgo de la NTC ISO 27005. Definir conceptos y contextualización del medio ambiente, identificación y estudio de riesgos a través de conocimientos, activos, amenazas, vulnerabilidades, probabilidad de ocurrencia e impacto. Para la estimación y el cálculo del riesgo se lleva a cabo el tratamiento más adecuado. Todo el trabajo se basa en un estudio de caso, con el objetivo de consolidar los conocimientos teóricos. Al final del curso el alumno estará capacitado para realizar un análisis cualitativo del riesgo en el entorno de su organización.

A quienes se destina

Directivos, técnicos y profesionales de la informática o áreas afines, que buscan el desarrollo de habilidades en la realización de análisis de gestión del riesgo en el ámbito de las Tecnologías de la Información y Comunicación, TIC. Profesionales de otras áreas pueden participar siempre y cuando posean conocimientos de las TIC, seguridad de la información y las normas ISO 27001 y 27002.

Convenciones utilizadas en el libro

Las siguientes son convenciones tipográficas usadas en este libro:

Itálico Indica los nombres de archivos y referencias bibliográficas relacionadas a lo largo del texto.

Indica ejemplos para una mejor comprensión de los conceptos presentados.

Indica una referencia complementaria disponible en internet.

Indica un alerta o precaución a tener en cuenta.

Indica cuestionamientos que estimulan la reflexión o presentan contenido de apoyo para la comprensión del tema tratado.

Indica un documento como referencia complementaria.

Sobre los autores de la versión portuguesa

Edson Kowask Bezerra profesional del área de seguridad de la información y gobierno de información, con más de quince años como auditor líder de calidad, investigador, director de proyectos y director técnico en varios proyectos de gestión de riesgos, la gestión de la seguridad de la información, continuidad del negocio, PCI, auditoría y recuperación de desastres en las grandes empresas de telecomunicaciones, financiera, energía, industria y empresas del sector del gobierno. Con amplia experiencia en las áreas de seguridad. También ha actuado como conferencista en importantes eventos en Brasil y también como instructor de formación en los temas de seguridad y gobierno. Es profesor y coordinador de cursos de postgrado en el área de seguridad de la información, la gestión integrada, la innovación y las tecnologías web. Hoy se desempeña como Coordinador Académico de Seguridad y Gobierno de las TI de la Escuela Superior de Redes.

Fabiano Alcántara Lima Magíster en Sistemas de Gestión, Especialista en Administración e Información y Sistemas Informáticos, su formación de base es en Ciencias de la Computación, Especialista en Gestión del Riesgo y proyectos con énfasis en Proyectos de Tecnología de la Información. Posee certificación en Project Management Professional por PMI y Microsoft Certified Technology Specialist en MS-Project 2007, con 12 años de experiencia en empresas nacionales y multinacionales grandes y medianas. Ha sido expositor, autor e investigador de temas de gestión de proyectos, gestión del riesgo, estrategia de negocio y gobierno de TI. Profesor en las áreas de gestión del riesgo y gestión de proyectos con MS-Proyecto en el programa MBA en gestión de proyectos de la Universidad Veiga de Almeida. Instructor de Dinsmore Associates en cursos en gestión de proyectos y preparación para la certificación PMP

Alexandre Cesar Motta Magíster en Administración con énfasis en planeación organizacional y gestión de recursos humanos de la PUC- Rio. MBA en Gerencia de Proyectos de la FGV-RJ. Economista de la PUC-Rio con más de 10 años de experiencia profesional en cargos de coordinación y dirección de importantes Instituciones de Educación Superior. Profesor de cursos de pregrado y posgrado en las áreas de marketing, recursos humanos, planeación organizacional y gerencia de proyectos. Cuenta con experiencia como facilitador en programas de entrenamiento y desarrollo de competencias, habilidades técnicas y gerenciales en la implementación de proyectos de consultoría en gestión de recursos humanos, gerencia de proyectos y organización de empresas.

Jacomo Dimmit Boca Piccolini, con estudios de postgrado en el Instituto de Computación y Economía de UNICAMP e Ingeniero de la Universidad Federal de São Carlos. Sirve como Coordinador Académico de las áreas de Seguridad y Gobierno de TI de la Escuela de Redes, ESR, de la Red Nacional de Investigación y Educación, RNP. Con más de 12 años de experiencia en seguridad, tiene certificaciones en materia de seguridad y gobernanza de TI. También es director de investigación de Dragon Research Group, Coordinador de Capacitación de FIRST.org, miembro del Consejo de ISACA Brasilia y profesor invitado en los cursos de postgrado en las disciplinas de la ciencia forense, sistemas de seguridad, manejo de incidentes, la creación y gestión CSIRT.

Sobre la autora de la versión adaptada y ampliada

Ingrid Patricia Páez Parra, Doctora en Ingeniería de Telecomunicaciones, Universidad de Cantabria. Ingeniera Eléctrica, Escuela Colombiana de Ingeniería. Ingeniera Industrial, Universidad de Cantabria. Experiencia en investigación, Universidad de Cantabria, Departamento de Ingeniería de Comunicaciones. Docente investigadora Universidad Pontificia Bolivariana, sede Medellín, Facultad de Ingeniería de Telecomunicaciones e Informática. Ha participado como Investigadora en proyectos con Colciencias en temas de pedagogía curricular y didáctica para la formación de técnicos, tecnólogos e ingenieros en telecomunicaciones. Autora de varios artículos y ponencias publicados en el ámbito nacional e internacional. Conferencista y ponente en diferentes eventos de carácter nacional e internacional. Actualmente trabaja como Profesora Asociada del Departamento de Ingeniería de Sistemas e Industrial de la Universidad Nacional de Colombia y es miembro como Investigadora del Grupo de Investigación GITUN.

Sobre la traducción para la versión adaptada y ampliada

Oscar Edwin Piamba Tulcán, Doctor en Ingeniería Mecánica de la Universidad Federal Fluminense, Magíster en Ingeniería Mecánica de la Universidad de los Andes con Especialización en Ciencias: Física de la misma Universidad e Ingeniero Mecánico de la Universidad Nacional de Colombia. Vinculado como profesor a la Facultad de Ingeniería de la Universidad Nacional de Colombia desde el año 2000, se desempeña como Director Nacional de Información Académica desde 2010. Participa como docente en los programas de Doctorado en Ingeniería Mecánica, en el Doctorado en Ciencia y Tecnología de Materiales y en los programas de maestría y pregrado en Ingeniería Mecánica y Mecatrónica.

Tabla de contenido

Capítulo

01

Introducción a la gestión del riesgo

Objetivos

Conceptualizar y comprender amenazas, vulnerabilidades y riesgos; conocer y utilizar la norma de gestión del riesgo; identificar las actividades del proceso de gestión del riesgo y los factores críticos para el éxito; identificar y definir las áreas necesarias para la gestión del riesgo

Conceptos

Amenazas, vulnerabilidades, probabilidad, riesgos, seguridad de información y gestión del riesgo.

Introducción

En las fases del ciclo de vida de cualquier actividad humana planeada convivimos con dos certezas básicas: lo que debe pasar (los objetivos) y lo que puede pasar (la incertidumbre).

La acción y la interacción de los objetivos con la incertidumbre dan origen al riesgo, que se presentan en el día a día de cualquier actividad desarrollada. Muchas veces, el riesgo está visible, siendo necesario implementar acciones para identificarlo; en otras situaciones el riesgo es resultado de acciones repentinas que escapan del control del ser humano, como en caso de eventos de causas naturales.

Diariamente vemos noticias en publicaciones de las más diversas áreas que destacan, enfatizando, los problemas relacionados a los riesgos tecnológicos de seguridad de la información: robos de los medios de *backup* y de *notebooks*, fuga o robo de números de tarjetas de crédito, manipulación indebida de registros electrónicos, robo de identidad y violación de propiedad intelectual.

Este capítulo abordará los conceptos fundamentales para la gestión del riesgo y presentará la norma ICONTEC NTC-ISO/IEC 27005:2008: Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información.

Ejercicio de nivelación - introducción a la gestión del riesgo

- ¿Cómo evalúa en su organización el proceso de gestión del riesgo?
- ¿Existen riesgos para los trabajos y actividades de su organización?

1.1 Tendencias en el área de la gestión del riesgo

Las Tecnologías de la Información y Comunicaciones, TIC, son indispensables en las organizaciones porque implican altos costos para su desarrollo y soporte, además de asociarsen a enormes riesgos de seguridad. La información es un activo de valor vital para el éxito y la prolongación en el mercado de cualquier organización. Las organizaciones presentan deficiencias en el manejo y en el aseguramiento de la información y en consecuencia de los sistemas que la procesan.

"Todas las organizaciones se enfrentan a factores internos y externos que generan incertidumbre sobre si serán capaces de alcanzar los objetivos, el efecto de esta incertidumbre es riesgo y es inherente a todas las actividades" [2], la seguridad absoluta no existe, pero se trata de reducir el riesgo a niveles asumibles, la seguridad de la información desde el enfoque de la gestión del riesgo implica identificar, evaluar y controlar los riesgos en la organización.

El riesgo cero no existe prácticamente en ningún caso, pero las organizaciones requieren de un proceso de seguridad de la información desde el enfoque de la gestión del riesgo, una evaluación del riesgo exhaustiva y adecuada en la organización tiene como resultado la reducción de pérdida, robo o corrupción de la información. La gestión del riesgo evalúa el daño resultante de una falla y la probabilidad de ocurrencia, estima el nivel de riesgo resultante y determina si el riesgo es aceptable o requiere de un tratamiento.

Las instituciones de normalización ofrecen a las organizaciones una serie de orientaciones sobre las mejores prácticas de seguridad, aunque existe un conjunto de herramientas, estándares, buenas prácticas por si solas que son difíciles y no presentan estructuradamente los diferentes componentes de la organización ni la manera como éstas se pueden integrar, es por ello, que se establece una metodología de gestión del riesgo que aborda esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad de la información, estructurada con directrices que llevan a cabo una guía de procesos que identifican las amenazas, evalúan las vulnerabilidades y probabilidades de ocurrencia y analizan los impactos, presentando un plan de tratamiento adecuado.

2 Kevin W. Knight, Presidente del grupo de trabajo de la ISO 31000

Elegir un estándar no es una tarea sencilla, esa labor tiene muchos factores a evaluar, entre ellos la semejanza de las normas, sin embargo cualquier ejercicio de la gestión del riesgo debe llevar a cabo estos procesos previstos por los principales estándares. Las metodologías de evaluación del riesgo implican un conjunto organizado de principios y normas, una metodología que describe métodos específicos constituyendo un marco genérico de la gestión. La evaluación del riesgo es un requisito obligatorio en la gestión de la seguridad.

Como conclusión la seguridad de la información requiere desarrollarse desde el enfoque de la gestión del riesgo, como un proceso de actividad continua de evaluación. Actualmente los organismos de estandarización están renovando las normas de gestión del riesgo como la NIST SP 800-30 del año 2012 y en Colombia la ratificación de la norma ISO 31000 en el año 2011 (estándar global sobre gestión del riesgo).

1.2 Conceptos fundamentales

- Norma ISO GTC 137. Gestión del riesgo. Vocabulario
  - Recomendaciones para el uso en normas.
  - Presenta las principales terminologías para el uso en actividades de gestión del riesgo.
- Esta terminología debe ser combinada con los términos presentados en las normas:
  - ICONTEC NTC-ISO/IEC 27001.
  - ICONTEC ISO/IEC 27002.

Es importante tener siempre en mente los siguientes conceptos:

- **Seguridad de la información:** es la protección de la información en relación con varios tipos de amenazas, a fin de garantizar la continuidad del negocio, minimizando los riesgos que puedan comprometerlo, y maximizando el retorno sobre las inversiones y las oportunidades de la organización. La seguridad de la información se logra mediante la implementación de un conjunto de controles: políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software.

La seguridad de información se logran mediante controles que deberán ser monitoreados, analizados y continuamente mejorados con el interés de atender a los objetivos del negocio, mitigando los riesgos y garantizando los preceptos de seguridad de la organización: Confidencialidad, Integridad, Disponibilidad, y Autenticidad, CIDA.

» **Amenaza:** es cualquier evento que pueda explotar las vulnerabilidades. Causa potencial de un incidente indeseado, que puede resultar en daños para los sistemas, personas o la propia organización. Las amenazas poden ser clasificadas en:

- Amenazas intencionadas
- Amenazas por acción de la naturaleza.
- Amenazas no intencionadas.

Son ejemplos de amenazas:

- Errores humanos
- Fallas de hardware
- Fallas de software
- Acciones de la naturaleza
- Terrorismo
- Vandalismo, entre otras

» **Vulnerabilidad:** es cualquier debilidad que puede ser explotada para comprometer la seguridad de sistemas de la información. Fragilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Para pensar

Amenaza versus Vulnerabilidad
Se entiende que la amenaza es el evento o incidente, mientras que la vulnerabilidad es la fragilidad que será explotada para que la amenaza se torne concreta. Las amenazas pueden asumir diversas formas, como hurto de equipos, medios y documentos, escucha no autorizada, incendio, inundación y radiación electromagnética, hasta fenómenos climáticos y sísmicos. Por ejemplo, un computador cuya clave sea del conocimiento de todos sufre amenazas como robo, destrucción o alteración de la información; la vulnerabilidad que permite que estas amenazas se concreten es justamente el hecho de que la clave es conocida por todos.

Tabla 1. Ejemplos de vulnerabilidad y amenazas

Vulnerabilidad	Amenaza
Falta de entrenamiento de funcionarios	Errores humanos
Interrupción en el servidor por quema de fuente	Falla de hardware
El sistema aplicativo acepta cualquier valor en sus campos	Falla del software
Inundación de la sala en virtud de las fuertes lluvias	Acciones de la naturaleza
Explosión provocada intencionalmente en el terminal de bus	Terrorismo
Maquina ATM destruida	Vandalismo

Los conceptos a continuación explican las actividades después de la identificación del riesgo y relacionadas a su tratamiento.

- **Riesgo:** combinación de probabilidad (probabilidad de que la amenaza se concrete) de que un evento indeseado ocurra y de sus consecuencias para la organización. Es la incertidumbre resultante de la combinación de la probabilidad de la ocurrencia de un evento y sus consecuencias. La pregunta "¿cuál es el riesgo?" genera una duda al respecto de la ocurrencia de algo incierto o inesperado. En seguridad de la información, esta incertidumbre reside en los aspectos tecnológicos involucrados, en los procesos ejecutados y, principalmente, en las personas que en algún momento interactúan con la tecnología y se involucran con los procesos.
- **Riesgos de seguridad de la información:** posibilidad de que una determinada amenaza explote las vulnerabilidades de un activo o de un conjunto de activos, perjudicando así a la organización.
- **Identificación del riesgo:** proceso para localizar, enumerar y caracterizar elementos de riesgo. Por menor que sea la probabilidad de ocurrencia de un riesgo, una determinada incertidumbre puede explotar una vulnerabilidad concretizando una amenaza. Para prepararse para eso es necesario conocer los riesgos de todo el ambiente, a través de la realización de un proceso formalizado de identificación del riesgo.
- **Impacto:** cambio adverso en el nivel obtenido de los objetivos de negocios. Consecuencia evaluada de los resultados con la ocurrencia de un evento en particular, en que determinada vulnerabilidad fue explotada, una amenaza ocurrió y el riesgo se concretizó. ¿Cuál fue el impacto de este evento en los negocios? ¿Cuánto se perdió? ¿La organización será responsabilizada?

¿Habrá multas? ¿Acciones legales serán impulsadas? ¿Habrá daños de imagen?

Imagine las siguientes situaciones hipotéticas:

1. En una Institución de Educación Superior, IES, un usuario con acceso a la información de los alumnos dejó su clave escrita en un papel después de renovarla. ¿Qué puede ocurrir? ¿Cuál es el impacto?
2. En plena preparación para el examen de admisión de una determinada institución los exámenes se filtran. ¿Cuál es el impacto si esta fuga ocurrió seis meses antes de la realización del examen? ¿Y si ocurrió en las 48 horas que anteceden a la realización del examen?

Ejemplos de impactos: pérdidas financieras, paralización de servicios esenciales, pérdida de confianza de los clientes, corte en el servicio de energía y falla de telecomunicaciones, entre muchos otros.

- **Estimación del riesgo:** proceso utilizado para atribuir valores a la probabilidad y consecuencias de un riesgo. La estimación del riesgo permite cuantificar o describir de forma cualitativa un riesgo, permitiendo a las organizaciones priorizar los riesgos de acuerdo con los criterios establecidos.
- **Acciones de modificación del riesgo:** acciones tomadas para reducir la probabilidad, las consecuencias negativas, o ambas, asociadas a un riesgo.
- **Comunicación del riesgo:** intercambio de información sobre el riesgo entre quien toma la de decisión y las otras partes interesadas.
- **Acciones para evitar el riesgo:** decisión de no involucrarse o reaccionar de forma que mitigue una situación de riesgo.
- **Retención del riesgo:** aceptación de la consecuencia de pérdida o beneficio de la ganancia asociada a un determinado riesgo.
- **Compartir el riesgo:** compartir con otra entidad la consecuencia por la pérdida o el beneficio de la ganancia asociada a un riesgo.

Ejercicio de refuerzo - conceptos fundamentales

» Durante una presentación sobre los conceptos de gestión del riesgo para la alta dirección de su organización, usted fue cuestionado sobre dos posibles amenazas existentes y sus riesgos. ¿Cómo respondería?
» En función de su respuesta para la alta dirección, le pidieron explicar los posibles impactos relacionados a estos riesgos. ¿Cómo respondería?

1.3 Principios de la gestión del riesgo

Para que la gestión del riesgo sea eficaz, conviene que una organización, en todos los niveles, atienda a los principios descritos a continuación.

a. La gestión del riesgo crea y protege el valor.
La gestión del riesgo contribuye a la realización demostrable de los objetivos y a la mejora de desempeño, referente a la seguridad y salud de las personas, a la conformidad legal y regulatoria, a la aceptación pública, a la protección del medio ambiente, a la calidad del producto, a la gerencia de proyectos, a la eficiencia en las operaciones, al gobierno y la reputación.

b. La gestión del riesgo es parte integrante de todos los procesos organizacionales.
La gestión del riesgo no es una actividad autónoma separada de las principales actividades y procesos de la organización. La gestión del riesgo hace parte de las responsabilidades de la administración y es parte integrante de todos los procesos organizacionales, incluida la planeación estratégica y todos los procesos de gestión de proyectos y gestión del cambio.

c. La gestión del riesgo es parte de la toma de decisiones.
La gestión del riesgo apoya a los tomadores de decisiones para que hagan selecciones consistentes, prioricen acciones y distingan entre formas alternativas de acción.

d. La gestión del riesgo aborda explícitamente la incertidumbre.
La gestión del riesgo explícitamente tiene en cuenta la incertidumbre, la naturaleza de esa incertidumbre, y cómo puede ser tratada.

e. **La gestión del riesgo es sistemática, estructurada y oportuna.**
Un abordaje sistemático, oportuno y estructurado para la gestión del riesgo contribuye para obtener eficiencia y resultados consistentes, comparables y confiables.

f. **La gestión del riesgo se basa en la mejor información disponible.**
Las entradas del proceso para realizar la gestión del riesgo están basadas en fuentes de información, tales como datos históricos, experiencias, retroalimentación de las partes interesadas, observaciones, previsiones y opiniones de especialistas. Entretanto, conviene que los tomadores de decisiones se informen y tengan en cuenta cualquier limitación de los datos o modelos utilizados, o la posibilidad de divergencias entre especialistas.

g. **La gestión del riesgo es hecha a la medida.**
La gestión del riesgo está alineada con el contexto interno y externo de la organización y con el perfil del riesgo.

h. **La gestión del riesgo considera factores humanos y culturales.**
La gestión del riesgo reconoce las capacidades, percepciones e intenciones del personal interno y externo, que pueden facilitar o dificultar la realización de los objetivos de la organización.

i. **La gestión del riesgo es transparente e inclusiva.**
La participación apropiada y oportuna de partes interesadas y, en particular, de los tomadores de decisión en todos los niveles de la organización asegura que la gestión del riesgo permanezca pertinente y actualizada. La participación también permite que las partes interesadas sean debidamente representadas y tengan sus opiniones contempladas en la determinación de los criterios del riesgo.

j. **La gestión del riesgo es dinámica, iterativa y capaz de reaccionar a los cambios.**
La gestión del riesgo continuamente percibe y reacciona a los cambios. A medida que pasan los eventos externos e internos, el contexto y el conocimiento se modifican, el monitoreo y el análisis crítico del riesgo son realizados, nuevos riesgos surgen, algunos se modifican y otros desaparecen.

k. **La gestión del riesgo facilita el mejoramiento continuo de la organización.**
Conviene que las organizaciones desarrollen e implementen estrategias para mejorar su madurez en la gestión del riesgo, de manera conjunta con todos los demás aspectos de su organización.

Estos principios de la gestión del riesgo deben ser los orientadores de esta noble actividad en el día a día de las organizaciones.

1.4 Normas de gestión de seguridad del riesgo

El área de seguridad de la información posee un conjunto de normas para ser utilizadas en las más diversas organizaciones, a fin de permitir una estandarización de los requisitos y procedimientos para la implementación de un Sistema de Gestión de Seguridad de la Información, SGSI.

ICONTEC: (Instituto Colombiano de Normas Técnicas y Certificación) es un organismo multinacional de carácter privado, sin ánimo de lucro, que trabaja para fomentar la normalización, la certificación, la metrología y la gestión de la calidad en Colombia. Está conformado por la vinculación voluntaria de representantes del gobierno nacional, de los sectores privados de la producción, distribución y consumo, el sector tecnológico en sus diferentes ramas y por todas aquellas personas jurídicas y naturales que tengan interés en pertenecer a él.

Norma ICONTEC NTC-ISO/IEC 27001:2006

- Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos
- Presenta y describe los requisitos que deben ser implementados en el establecimiento de un SGSI.

Norma ICONTEC NTC-ISO/IEC 27002:2007

- Tecnología de la información. Técnicas de seguridad. Código de práctica para la de gestión de seguridad de la información
- Presenta las mejores prácticas para una gestión adecuada de la seguridad de la información.

En el campo de la normalización, la misión del ICONTEC es promover, desarrollar y guiar la aplicación de Normas Técnicas Colombianas, NTC

y otros documentos normativos, con el fin de alcanzar una economía óptima de conjunto, el mejoramiento de la calidad y también facilitar las relaciones cliente-proveedor en el ámbito empresarial nacional o internacional.

Pudiendo ser aplicadas a cualquier ambiente de una organización (particularmente al ambiente de las TI), estas normas destacan la necesidad de las organizaciones de poseer una gestión del riesgo estructurada, con la estandarización de procesos y requisitos de gestión del riesgo.

En 1995, la comisión de estandarización de Australia y Nueva Zelandia lanzó la primera norma tratando el tema: AS/NZS 4360. Gestión del riesgo. La norma establece un proceso de gestión del riesgo ampliamente aceptado, habiendo sido actualizada en 1999 (AS/NZS 4360:1999). En 1996, la Organización Internacional de Normalización, ISO, creó un grupo de trabajo basado en la AS/NZS 4360 para elaborar un proyecto de gestión del riesgo, que pasó por diversos problemas y solo fue concluido en 2009.

La norma ICONTEC NTC-ISO 31000. Gestión del riesgo. Principios y directrices fue lanzada en 2009 por la ISO e inmediatamente adoptada por el ICONTEC.

Esta norma brinda los principios y directrices genéricas para cualquier industria o sector. En el mismo año fue lanzada la norma ICONTEC ISO-GTC 137. Gestión del riesgo. Vocabulario. Esta presenta las definiciones de términos genéricos relacionados con la gestión del riesgo. Cuando se pretende hacer referencia a un concepto de gestión del riesgo, debe ser utilizada la definición de la norma ICONTEC ISO-GTC 137. Gestión del riesgo. Vocabulario. Según ICONTEC:

"Esta guía brinda las definiciones de términos genéricos relacionados con la gestión del riesgo. Destinada a incentivar una comprensión mutua y consistente, un abordaje coherente en la descripción de las actividades relativas a la gestión del riesgo y la utilización de terminología uniforme de gestión del riesgo en procesos y estructuras para la gerencia del riesgo".

En febrero de 2011 fue lanzada la norma "ICONTEC NTC-ISO/IEC 31010. Gestión del riesgo. Técnicas para el proceso de evaluación del riesgo" que debe ser usada con apoyo en la norma "ICONTEC NTC-ISO 31000 Gestión del riesgo. Principios y directrices". La norma describe las diversas técnicas y herramientas de análisis del riesgo, brindando orientaciones sobre la selección y aplicación de técnicas sistemáticas para el proceso de evaluación del riesgo.

Este grupo de normas de la serie 31000 busca atender a cualquier tipo de ambiente de una organización. Proporcionan, por tanto, una concepción amplia y genérica de la gestión del riesgo, siendo aplicadas para evaluar y tratar cualquier tipo de riesgo corporativo. Durante el desarrollo de estas normas, la norma "ICONTEC NTC-ISO/IEC 27005:2008 Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información" fue publicada en 2008 por el grupo de trabajo específico de tecnología de la información. Esta norma fue desarrollada basada en los estudios de la ISO 31000, y por lo tanto atiende a los requisitos y al proceso de gestión del riesgo. La ISO/IEC 27005 hace parte del conjunto de normas de la serie 27000, sobre el SGSI, donde son incluidas las normas ISO/IEC 27001 y 27002. Esta norma presenta las mejores prácticas y posibilita profundizar en aspectos exclusivos de seguridad de la información, mientras la ISO 31000 es más genérica y contempla todos los sectores.

El enfoque de este curso está en la norma "ICONTEC NTC-ISO/IEC 27005:2008. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información". Los conceptos, procesos, y actividades presentados se adecuan al que propone a la norma "ICONTEC NTC ISO 31000. Gestión del riesgo. Principios y directrices", pudiendo ser aplicados en cualquier otra área que no sea de TI.

La siguiente tabla presenta un resumen comparativo entre estas normas:

Tabla 2. Resumen comparativo entre las normas.

Norma	Titulo	Objetivo	Observación
27001	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos	Especificar los requisitos para establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar un SGSI documentado en el contexto de los riesgos de negocio globales de la organización. Especifica requisitos para la implementación de controles de seguridad personalizados para las necesidades individuales de organizaciones o de sus partes. Cubre todos los tipos de organización (emprendimientos comerciales, agencias gubernamentales, organizaciones sin fines lucrativos, entre diversas otras).	Tratar más específicamente de directrices y principios para un sistema de gestión de seguridad de la información.
27002	Tecnología de la información. Técnicas de seguridad. Código de práctica para la de gestión de seguridad de la información	Establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información. Los objetivos definidos en esta norma establecen directrices generales para las metas y mejores prácticas para la gestión de la seguridad de la información.	Enfocada a controles de seguridad.
27005	Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información	Presenta un sistema de gestión del riesgo de seguridad de la información con énfasis en tecnología de la información.	Aclara como realizar la gestión del riesgo de seguridad de información.
31000	Gestión del riesgo. Principios y directrices	Norma que presenta principios y directrices básicas para la gestión del riesgo en general en cualquier tipo de ambiente.	Editada en 2009, de este año en delante las demás normas de gestión del riesgo deben estar alineadas a esta.
31010	Gestión del riesgo. Técnicas para el proceso de evaluación del riesgo	Describe las diversas técnicas y herramientas de análisis del riesgo.	Editada en 2012.
GUIDE 73	Gestión del riesgo. Vocabulario	Presenta las definiciones de términos genéricos relacionados con la gestión del riesgo.	Editada en 2009.

1.5 Norma ICONTEC NTC ISO/IEC 27005:2008

La norma "ICONTEC NTC-ISO/IEC 27005:2008. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información" fue publicada en julio de 2008 y presenta las directrices para la gerencia del riesgo de seguridad de información. Emplea los conceptos de norma ICONTEC NTC-ISO 27001:2005, que especifica los requisitos de sistemas de gestión de la seguridad de la información.

Esta norma describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión. Presenta prácticas para gestión del riesgo de la seguridad de la información. Las técnicas en ella descritas siguen el concepto, los modelos y los procesos globales especificados en la norma ICONTEC NTC-ISO/IEC 27001, además de presentar la metodología de evaluación y tratamiento de los riesgos requeridos por la misma norma.

Partiendo del principio de que la gestión del riesgo es un proceso cíclico y continuo, la norma está dividida en secciones y anexos. Las secciones contienen la información del proceso y de las actividades necesarias para su ejecución. Existen 12 secciones en total: las secciones 1 a 4 tratan las referencias y la estructura de la norma, y las secciones 5 y 6 presentan una visión general del proceso de gestión del riesgo. Las secciones a partir de la 7 tratan específicamente del proceso de gestión del riesgo. Los seis anexos son identificados de A a la F y traen información adicional y ejemplos.

En las sesiones de 7 a 12 las actividades de gestión son presentadas de acuerdo con la siguiente estructura:

- **Entrada:** se refiere a los insumos y premisas necesarias para la realización de la actividad.
- **Acción:** descripción de la actividad, siempre acompañada del "conviene"
- **Directrices para implementación:** directrices necesarias para la realización de la acción, es decir, los detalles de cómo se puede realizar la acción. Estas directrices deben ser adaptadas a cada tipo de organización. También están acompañados del "conviene".
- **Salida:** presenta los resultados que se deben alcanzar y que servirá para generar evidencia.

Este curso utiliza el proceso de gestión del riesgo estandarizado contenido en la norma ICONTEC NTC ISO/IEC 27005.

1.6 Visión general de la gestión del riesgo

La gestión del riesgo son actividades formalizadas y coordinadas para controlar y dirigir un conjunto de instalaciones y personas con relaciones y responsabilidades entre ellos y externamente, en relación a los riesgos en los negocios desde la perspectiva de la seguridad de la información.

Definición del contexto;

- Análisis/Evaluación del riesgo;
- Tratamiento del riesgo;
- Aceptación del riesgo;
- Comunicación del riesgo;
- Monitoreo y análisis crítico;
- Ciclo de mejora continua PHVA.

La Tabla 3 muestra las principales actividades de la gestión del riesgo de seguridad de la información.

Tabla 3. Principales actividades de gestión de seguridad de la información.

Proceso del SGSI	Proceso de gestión del riesgo de seguridad de la información
Planear	» Definición del contexto » Análisis/Evaluación del riesgo » Definición del plan de tratamiento del riesgo » Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo continuo y análisis crítico del riesgo
Actuar	Mantenimiento y mejora del proceso de gestión del riesgo de seguridad de la información

Sugerencia de lectura: Bernstein, Peter. Desafío a los dioses: la fascinante historia del riesgo. Editora Campus, 1997.

En su libro "Desafío a los dioses: la fascinante historia del riesgo", Peter Bernstein nos ofrece un detallado análisis histórico de la evolución del control y la predicción de los riesgos por la humanidad desde la Grecia antigua. Según el autor, somos dotados de un elevado potencial técnico para la prevención de pérdidas y ganancias, aunque el comportamiento de los agentes sea impredecible. En sus palabras: "...pase lo que pase y a pesar de todos nuestros esfuerzos, los seres humanos no tienen el conocimiento completo sobre las leyes que definen el orden del mundo objetivamente existente". Por lo tanto, el autor nos descalifica como "predictores perfectos" del futuro.

Bernstein aún dice que "Cuando los inversores compran acciones, los cirujanos realizan operaciones, ingenieros diseñan puentes, los empresarios abren sus negocios y los políticos se postulan para cargos electivos, el riesgo es un socio ineludible. Sin embargo, sus acciones revelan que el riesgo no necesita ser tan temido: administrar el riesgo es sinónimo de desafío y oportunidad" El riesgo hace parte de nuestra vida diaria, de modo que necesitamos conocerlo para tratarlo y extraer de este nuevas oportunidades.

Sin lugar a dudas es importante el papel que la tecnología de la información ejerce en la sociedad para que ésta alcance sus objetivos. La integración del ambiente tecnológico, caracterizado por la complejidad y la interdependencia, produce contextos muchas veces hostiles que propician ataques cada vez más frecuentes a la seguridad de la información, exigiendo repuestas cada vez más rápidas de las organizaciones. A este cuadro se suman nuevas obligaciones legales, de protección de la privacidad y el gobierno corporativo, generando la necesidad de las organizaciones de gestionar más eficazmente su infraestructura tecnológica.

Para hacer frente a estas nuevas amenazas y demandas, las organizaciones deben desarrollar una actitud proactiva, anticipándose a conocer sus debilidades y vulnerabilidades. Esto puede lograrse mediante la adopción de un proceso formal de gestión del riesgo de seguridad de la información, que permita a la organización establecer un nivel de riesgo aceptable.

Para eso es necesario un enfoque sistemático de la gestión del riesgo, que variará según el negocio de cada organización, así como el nivel del riesgo aceptable establecido por la dirección de cada organización.

Riesgo aceptable es el grado de riesgo que la organización está dispuesta a aceptar para el logro de sus objetivos estratégicos.

Ejercicio de refuerzo - visión general

» En su organización, ¿cuál sería el "riesgo aceptable" en el desempeño de sus actividades? Explique.

Aumentar la capacidad de gestionar el riesgo y optimizar el retorno son acciones integrantes de un enfoque sistémico, que proporciona un proceso formal para la mejora de la capacidad de identificación y evaluación del riesgo. Este enfoque debe ser coherente con los objetivos de la organización, teniendo en cuenta sus necesidades específicas, de conformidad con los requisitos de seguridad de la información. Para eso, el enfoque de la gestión del riesgo de seguridad de la información debe ser:

» Continua;
» Realizada en el momento oportuno;
» Repetitiva;
» De acuerdo con el ambiente de la organización;
» Ajustado al proceso de gestión del riesgo corporativos;
» De acuerdo con los requerimientos del negocio;
» Respaldada por la alta dirección.

Basado en el concepto amplio de que el proceso de gestión se compone de actividades coordinadas y formalizadas para controlar y dirigir una organización, formado por sus instalaciones y personal, con relaciones y responsabilidades entre sí y con agentes externos, se puede deducir que la gestión del riesgo es compuesta de actividades formalizadas y coordinadas para controlar y dirigir un conjunto de instalaciones y personas con relaciones y responsabilidades entre ellos y con el ambiente externo, en cuanto a los riesgos en los negocios desde la perspectiva de la seguridad de la información.

La Figura 1, presenta una visión del proceso de gestión del riesgo de seguridad de la información de acuerdo a la norma ICONTEC NTC-ISO/IEC 27005.

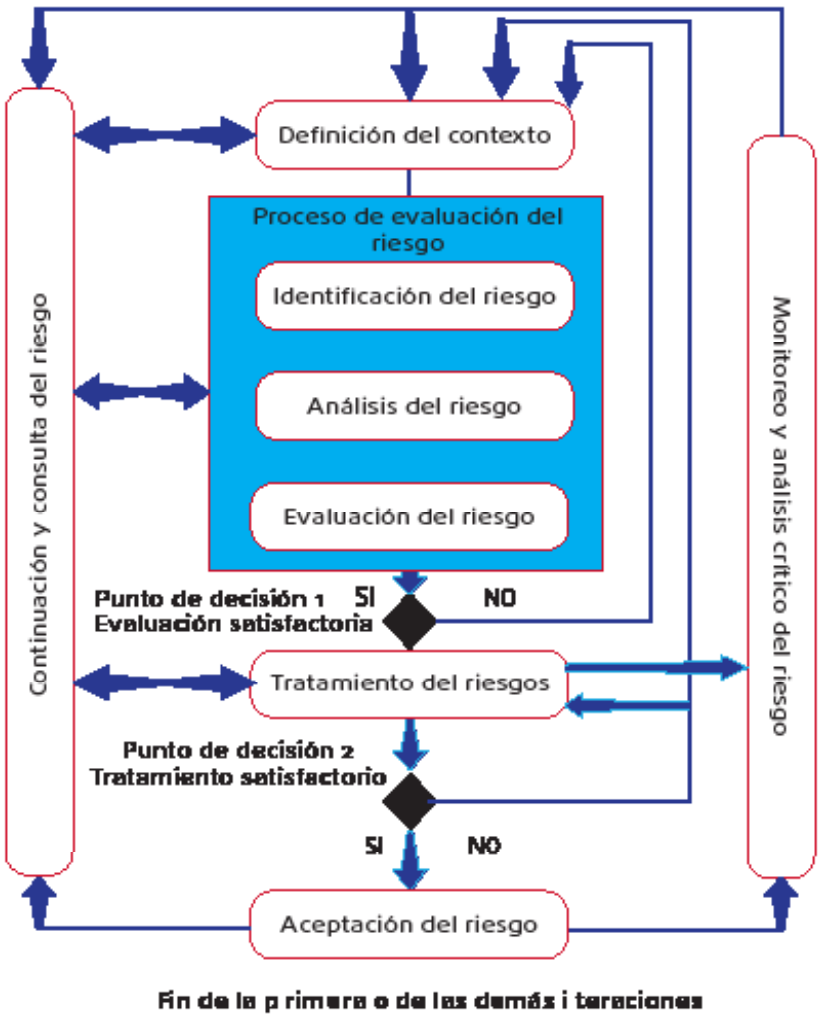


Figura 1.
Proceso de gestión del riesgo de seguridad de la información.

El proceso consta de seis grandes grupos de actividades:

- Definición del contexto;
- Análisis/Evaluación del riesgo;
- Tratamiento del riesgo;
- Aceptación del riesgo;
- Comunicación del riesgo;
- Seguimiento y análisis crítico.

Como puede verse en la Figura 1, el ciclo de vida de la gestión del riesgo de seguridad de la información es iterativo, donde la gestión se desarrolla de manera incremental, a través de una sucesión de iteraciones, y cada iteración libera una entrega (salida) para la siguiente, minimizando tiempo y esfuerzo.

- **Definición de contexto:** dentro del proceso, la definición de contexto es responsable de definir el ambiente, alcance, criterios de evaluación, y otros ajustes.
  Esta etapa es esencial para el equipo que lleva a cabo la gestión del riesgo de conocer toda la información sobre la organización.
- **Análisis/Evaluación del riesgo:** la siguiente iteración es de análisis y evaluación del riesgo, lo que permitirá la identificación del riesgo y la determinación de las acciones necesarias para reducir el riesgo a un nivel aceptable.
- **Tratamiento del riesgo:** los controles necesarios para el tratamiento del riesgo se definen a partir de los resultados obtenidos del análisis y la evaluación del riesgo. La norma ICONTEC NTC-ISO/IEC 27001 especifica los controles que deberán ser implementados.
- **Aceptación del riesgo:** asegura los riesgos asumidos por la organización, es decir, el riesgo que por alguna razón no será tratado o será tratado parcialmente. Estos se denominan riesgos residuales, cuya clasificación en esta categoría deberá justificarse.
- **Comunicación del riesgo:** En esta etapa se informa el riesgo y la forma como será tratado, para todas las áreas operacionales y sus gestores.
- **Seguimiento y análisis crítico:** son las actividades de acompañamiento de los resultados, implementación de controles y análisis crítico para el mejoramiento continuo del proceso de gestión del riesgo.

Todos estos pasos se detallan en los apartados siguientes.

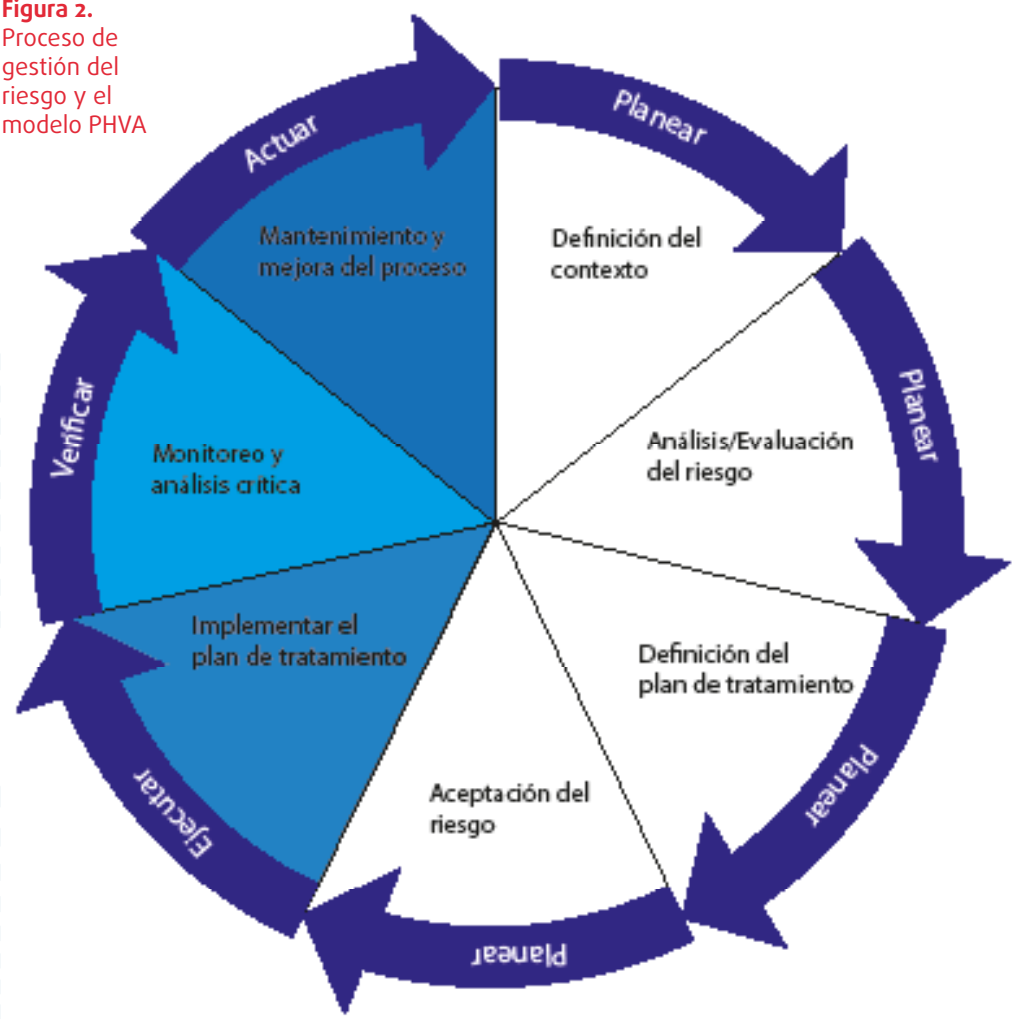
La norma ICONTEC NTC-ISO/IEC 27001 especifica que los controles implementados en el alcance, los límites y el contexto del SGSI deben basarse en el riesgo. Este requisito deberá cumplirse mediante la aplicación del proceso de gestión del riesgo de seguridad de la información.

En un entorno SGSI, la definición del contexto, el análisis y la evaluación del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo forman parte de la fase "Planear" del ciclo de mejora continua PHVA. La fase "Hacer" del SGSI es la implementación de con-

troles para manejar los riesgos al nivel aceptable para la organización. La fase "Verificar" del SGSI, a su vez, incluye las acciones de revisión. Por último, la fase "Actuar" comprende las acciones necesarias para ejecución, incluyendo la re-aplicación del proceso de gestión del riesgo de seguridad de la información.

Podemos resumir de la siguiente manera las actividades principales de la gestión del riesgo de seguridad de la información:

Figura 2.
Proceso de gestión del riesgo y el modelo PHVA



Ejercicio de refuerzo – PDCA

» Explique cómo la fase de planeación (PHVA) del proceso SGSI es realizada en el proceso de gestión del riesgo de seguridad de la información.

1.7 Factores críticos para el éxito

La gestión del riesgo de seguridad de la información es llevada a cabo por las organizaciones en la búsqueda de ventajas competitiva para los negocios. Es crucial para demostrar a las partes interesadas, una actitud de seguridad en la gestión de los riesgos relacionados con la protección de los activos de la información.

Los factores críticos del éxito están relacionados con los beneficios que se deben alcanzar por las organizaciones, dependiendo de la naturaleza de cada organización. Para lograr estos beneficios es necesario realizar las etapas que involucran los factores críticos para el éxito. Como ejemplos de estos factores podemos mencionar:

» **Implicación y participación de la alta dirección en el proceso:** es esencial para el éxito de cualquier proyecto que la dirección esté involucrada y comprometida con el desarrollo y éxito de acuerdo con los objetivos estratégicos definidos.
» **Comunicación y formación:** todo el proceso debe ser comunicado a todas las partes implicadas antes de su comienzo, durante su desarrollo y después de su conclusión, con la presentación de los resultados obtenidos y los objetivos conseguidos. En un proceso de gestión del riesgo todos los participantes deben estar involucrados, y para eso es necesario llevar a cabo una campaña de concientización y formación.
» **Definición de objetivos:** el establecimiento de objetivos contribuye de manera decisiva a la consecución de las metas de gestión del riesgo.
» **Funciones y responsabilidades definidas:** todos los miembros de las partes involucradas deben conocer sus funciones y responsabilidades durante todo el proceso de gestión del riesgo de seguridad de la información.
» **Integración con la gestión de seguridad de la información:** las actividades de gestión del riesgo deben estar totalmente integradas a las actividades del SGSI.

En el desarrollo de este curso se analizarán los factores críticos de éxito que pertenecen a cada etapa de la gestión del riesgo de seguridad de la información.

1.8 Áreas de conocimiento necesarios

Para mejorar la aplicación del proceso de gestión del riesgo es importante que los profesionales involucrados posean un perfil con conocimientos en diversas áreas, lo que permite la identificación de amenazas y vulnerabilidades en cualquier ambiente organizacional.

El equipo responsable de llevar a cabo el análisis del riesgo preferentemente debe tener los siguientes perfiles:

- **Técnico:** ayuda en el cumplimiento de las demandas de varias áreas técnicas de la organización, incluyendo las áreas de hardware, software, sistemas operativos, infraestructura y aplicaciones web, entre otros.
- **Negocios:** auxilia al equipo en la compresión precisa de los negocios de la organización y sus múltiples procesos, además de tener importancia en el cálculo de los impactos.
- **Legislación:** perfil enfocado hacia la comprensión de los aspectos legales y normativos con los cuales la organización analizada necesita alinearse.
- **Proceso:** permite la comprensión de los procesos y a través de su análisis identifica posibles amenazas y vulnerabilidades, lo que contribuye al desarrollo de planes de gestión y tratamiento del riesgo.

Estos son algunos ejemplos de perfiles o conocimientos necesarios para el análisis del riesgo. El tipo de organización y sus objetivos de negocio indican los perfiles que son realmente importantes para componer el equipo de trabajo. No hay necesidad de un profesional para cada perfil citado, porque el conocimiento se puede encontrar en un mismo profesional. El número de empleados asignados será determinado por el alcance de los análisis y el plazo.

Lectura complementaria

- Sesiones 4, 5 y 6 de la ICONTEC NTC- ISO/IEC 27005.
- Ítem 4 de la Norma Complementaria de Gestión del riesgo de seguridad de la información y comunicaciones. GRSIC, DSIC/GSI/PR: http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf
- *Enterprise Risk Management: Past, Present and Future:* http://www.casact.org/education/erm/2004/handouts/kloman.pdf
- *Interdisciplinary Risk Management:* http://www.riskinfo.com/rmr/rmrjun05.htm
- Cuatro consejos para una gestión eficaz de los riesgos: http://cio.uol.com.br/gestao/2009/07/03/quatro-dicas-para-a-boa-gestao-de-riscos/
- AS/NZS 4360: http://www.standards.org.au/Default.aspx
- Historia de la AS/NZS 4360: http://www.riskinfo.com/rmr/rmr-septoo.htm

Lo aprendido

- Concepto de gestión del riesgo.
- Visión general de la gestión del riesgo.
- Factores críticos de éxito.

Capítulo

02

Contexto de la gestión del riesgo

Objetivos

Conceptualizar y definir el contexto del ambiente de gestión del riesgo, identificar el alcance y las actividades de definición de criterios en el proceso de gestión del riesgo.

Conceptos

Contexto, alcance, límites y criterios

Introducción

Al iniciar cualquier tipo de trabajo, la primera actividad que debe realizarse es conocer el ambiente en que se desarrollará el trabajo, las personas que de alguna manera irán a interactuar, lo que será desarrollado, en resumen, "conocer el terreno" para saber conducir el avance de los trabajos.

En las actividades que involucran la gestión del riesgo de seguridad de la información la definición del contexto es la parte inicial y tiene como objetivo permitir el conocimiento del ambiente de la organización.

Ejercicio de nivelación - contexto

» En su entender, ¿cuál es el contexto actual de su organización?

2.1 Procesos de gestión del riesgo de seguridad de la información

En la sesión anterior fue presentada la visión general del proceso de gestión del riesgo. Es necesario que el conocimiento de la secuencia de las fases del proceso haga parte del día a día de los profesionales que intervienen en la gestión del riesgo.

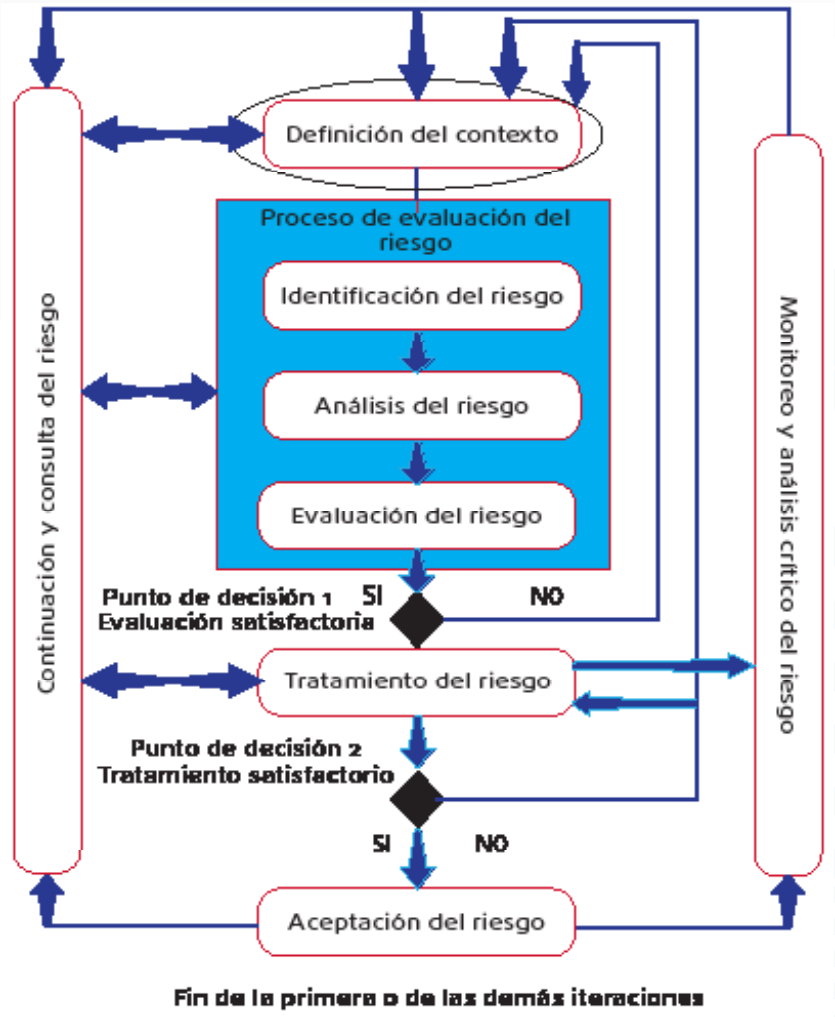


Figura 3. Definición del contexto.

Para realizar esta actividad, los profesionales deberán tener acceso a toda la información sobre la organización, permitiendo así un amplio conocimiento acerca de las especificaciones de la organización.

2.2 Contexto

Es necesario entender el significado conceptual de "contexto" y su aplicación en la gestión del riesgo. En la búsqueda de su significado en los diccionarios, se encuentra, entre otras definiciones, que contexto es un

sustantivo masculino, que significa "interrelación de las circunstancias que acompañan a un hecho o una situación."

Así, al referirnos al "contexto" queremos en realidad tratar la totalidad de las circunstancias que hacen que sea posible, condicionan o determinar la realización de un texto, proyecto, actividad o incluso un evento de seguridad. En otras palabras, contexto es el conjunto de circunstancias que se relacionan de alguna manera con un determinado acontecimiento. Es la situación general o el ambiente a que está siendo referido a un determinado asunto.

Llamamos contextualización a la actividad de mapear todo el ambiente que rodea al evento en cuestión. En el proceso de gestión del riesgo esta es la primera actividad a realizar.

De acuerdo con la norma ICONTEC NTC-ISO 31000 el contexto puede ser analizado desde dos aspectos:

- **Contexto externo:** es el ambiente externo en el cual la organización se encuentra y busca lograr sus objetivos (ambiente cultural, financiero reglamentario, tecnológico, económico, competitivo, entre otros).
- **Contexto interno:** es el ambiente interno, en el cual la organización busca alcanzar sus objetivos (gobierno, estructura organizativa, políticas, objetivos, competencias, sistemas de información, cultura organizacional, normas, directrices, entre otras.)

2.3 Establecimiento del contexto

De acuerdo con la norma ICONTEC NTC ISO/IEC 31000, en el momento en que la organización establece su contexto ella:

- Articula sus objetivos.
- Define los parámetros internos y externos.
- Define el alcance y los criterios de riesgo de todo el proceso de gestión del riesgo.

De acuerdo con la norma ICONTEC NTC-ISO/IEC 31000, cuando la organización establece su contexto ella articula sus objetivos, definiendo parámetros internos y externos que se deben tener en cuenta para realizar la gestión del riesgo, y define el alcance y los criterios del riesgo para todo el proceso de gestión del riesgo.

2.4 Contexto de la norma ICONTEC NTC-ISO/IEC 27005

La sección 7 de la norma ICONTEC NTC-ISO/IEC 27005 se refiere a las actividades que deben ser desarrolladas durante la fase de contexto de la gestión del riesgo. Estas actividades deben ser desarrolladas por el equipo de gestión del riesgo responsable, siendo realizadas mediante interacciones con los profesionales de la organización evaluada a través de:

- Presentación de la organización;
- Entrevistas con los directores, gerentes, técnicos y usuarios;
- Cuestionarios.

La sección 7 de esta norma está organizada de la siguiente manera:

- Sección 7.1. Consideraciones iniciales: el propósito de hacer la contextualización;
- Sección 7.2. Criterios básicos: criterios de evaluación;
- Sección 7.3. Alcance y límites: la importancia de definir el alcance y los límites de la gestión del riesgo;
- Sección 7.4. Organización para la gestión del riesgo de seguridad de la información: organización y responsabilidades del proceso de gestión del riesgo;
- Apéndice A. Informativo: detalles para definir el alcance y las restricciones que pueden impactar en los trabajos.

2.5 Definiendo el contexto

Al comenzar el trabajo de gestión del riesgo se debe primero hacer un levantamiento de toda la información relevante sobre el ambiente donde será ejecutado el análisis del riesgo. Debe quedar claro, incluso la comprensión sobre las actividades de la organización y los propósitos que llevó a la gestión del riesgo de seguridad de la información.

Son ejemplos de estos propósitos:

- **Soporte al SGSI:** la organización optó por implementar un SGSI y para eso debe realizar la gestión del riesgo de seguridad de la información como un requisito obligatorio.
- **Cumplimiento legal:** respuesta a una determinación legal o normativa. Ej.: bancos, operadoras de tarjetas de crédito.
- **Plan de continuidad de negocios:** necesaria para la preparación del plan que tiene como objetivo estructurar la forma en que la organización se enfrentará a un evento catastrófico. Para que no ocurra un impacto significativo en el negocio se requiere llevar a cabo un proceso de gestión del riesgo.
- **Plan de respuesta a incidentes:** para que la organización pueda tener su plan de respuestas a los incidentes es necesario el conocimiento de sus riesgos y vulnerabilidades.

En general, la comprensión de los propósitos de la implementación de la gestión del riesgo posibilita una visión de la importancia de esta actividad para los negocios de la organización. En la norma ICONTEC NTC-ISO/IEC 27005 el propósito hace parte de las directrices para la implementación de la actividad de definir el contexto: ver 7.1. Consideraciones generales.

Ítems para la identificación

Al analizar el ambiente de la organización, el equipo de analistas debe identificar los elementos que caracterizan a la organización y contribuyen a su desarrollo. El análisis de la organización debe contener al menos los siguientes ítems.

Tabla 4. Ítems para el análisis de la organización.

Ítems para la identificación	Ejemplos de preguntas
El objetivo principal de la organización	¿Cuál es el propósito de la organización? ¿Cuáles son sus objetivos?
El Negocio	¿Cuál es su negocio? ¿Cuál es el propósito de lo que se produce/desarrollado?
La misión	¿Cuál es su misión? ¿Para que existe? ¿Lo que ella se propone a hacer? ¿Para quién?
La visión de futuro	¿Cuál es su visión del futuro? ¿Qué se espera de ella en el tiempo?

Continuación tabla 4. Ítems para el análisis de la organización.

Ítems para la identificación	Ejemplos de preguntas
Los valores	¿Cuáles son sus valores? ¿Cómo se muestran?
La estructura organizacional	¿Cómo está organizada y estructurada? ¿Y la seguridad de la información? ¿Y las responsabilidades por la seguridad?
El organigrama	¿Cuál es su organigrama? ¿Quién es quién en el sector que trabaja? ¿Hay zona de seguridad de la información?
Las estrategias	¿Cuáles son sus principales estrategias de negocios? ¿Y de seguridad de la información?
Los productos	¿Cuáles son sus productos? ¿Cuál es el principal producto de apalancamiento de los negocios?
Los socios	¿Quiénes son sus socios? ¿Cómo se eligen? ¿Cómo colaboran? ¿Cómo es la relación de la seguridad de la información a ellos? ¿Cuáles son las obligaciones de seguridad de la información?
Los terceros	¿Quién son los terceros? ¿Cómo se eligen? ¿Cómo colaboran? ¿Cómo es la relación de la seguridad de la información con ellos? ¿Cómo es el contrato? ¿Cuáles son las obligaciones de seguridad de la información?
Las instalaciones	¿Cómo se divide el personal de la organización? ¿Dónde están los servidores? ¿Existe algún mecanismo para prevenir un incendio? ¿Cómo es hecha la protección física? ¿Cómo son los accesos?
Los funcionarios	¿Cómo son contratados? ¿Hay capacitación en seguridad de la información? ¿Cómo se contratan?

Ejercicio de refuerzo - definiendo el contexto

- ¿Cuál es el propósito de su organización? Explique.
- ¿Cuál debería ser uno de los objetivos que deben conducir a la gestión del riesgo de seguridad de la información en su organización? Justifique.

2.6 Definiendo alcance y límites

Para hacer frente a la complejidad de la definición del alcance, se recomienda escribirlo por tópicos, asegurándose de que todos los puntos fueron incluidos y no hay dudas, principalmente entre la comprensión del equipo de gestión del riesgo y la organización.

Es importante que la organización defina el alcance y los límites de la gestión del riesgo de seguridad de la información. Pero, ¿qué es el alcance?

El alcance es la forma en que se describen los límites del proyecto, su cobertura, sus resultados y sus entregables. Es el propósito, el objetivo, la intención o el propósito de la gestión del riesgo. Si el alcance es turbio, o deja espacio para la interpretación, será difícil para el equipo de la gestión del riesgo identificar los límites de su trabajo. Por lo tanto, el alcance debe ser claro, bien definido y comprendido por el equipo y la organización. De esta manera, con el alcance y los límites identificados, el equipo de análisis y la organización serán capaces de aumentar los bienes, personas, procesos y las instalaciones que estarán involucrados en la actividad de análisis y evaluación del riesgo.

Al definir el alcance, la organización deberá tener en cuenta los objetivos que deben ser alcanzados con el análisis/evaluación (propósito). Para eso deben ser considerados:

- Los objetivos y políticas de la organización;
- Estructura y funciones de la organización;
- Procesos de negocios;
- Activos;
- Expectativas;
- Restricciones.

Es importante considerar las restricciones que afectan a la organización e influyen en la orientación de seguridad de la información. Algunas de estas restricciones pueden afectar el alcance, por lo que el equipo debe estar preparado para identificar y determinar la influencia que tendrán en el alcance. Algunos ejemplos de restricciones:

- Restricciones técnicas.
- Restricciones financieras.
- Restricciones ambientales.
- Restricciones temporales (el tiempo es un factor determinante).
- Restricciones organizacionales.

Existen muchas otras restricciones que variarán en función del tipo o del negocio de la organización, así como también variarán la influencia de estas restricciones a la gestión del riesgo. El apéndice A de la norma ICONTEC NTC-ISO/IEC 27005 presenta y detalla estas restricciones, siendo una lectura obligatoria para una mejor comprensión. Es necesario evaluar la complejidad del alcance y hacer un desglose de sus objetivos, para que no exista ninguna duda acerca de su amplitud.

Ejemplos de alcance y límites:

- Una aplicación de las TI.
- La infraestructura de las TI.
- Un proceso de negocio.
- El departamento de las TI.
- Una filial.
- El sistema de internet *banking* de una institución financiera.
- El servicio de correo electrónico de la organización.
- El proceso de control de acceso físico de la organización.
- El *datacenter* de la organización.
- La infraestructura que atiende a los servicios ADSL de una operadora.
- El servicio de *callcenter*.
- El sistema logístico de distribución de las pruebas de licitación nacional.
- La intranet de la organización.

Ejercicio de refuerzo - definiendo el alcance y límites

- ¿Qué propósitos deben ser considerados en su organización para definir el alcance? Justifique.
- Cite una restricción técnica y organizacional que pueda existir en su organización. Justifique.

2.7 Criterios para la evaluación del riesgo

La palabra criterio del griego *Kriterion* y del latín criterio, significa establecer un patrón que sirve de base para que las cosas y las personas puedan ser comparadas y juzgadas.

Los criterios para la evaluación del riesgo se utilizan para evaluar los riesgos de seguridad y deben considerar:

- El valor estratégico del proceso;
- La criticidad de los activos;
- El histórico de ocurrencia de los eventos de seguridad;
- El valor del activo para el proceso;
- La probabilidad de ocurrencias y otros, de acuerdo a la organización y el alcance.

Los criterios también se utilizarán para establecer prioridades para el tratamiento del riesgo.

Ejemplo:

En un ambiente que posee una sala utilizada para el almacenamiento de papel y con un precario sistema de prevención y extinción de incendios, el riesgo de un incendio puede ser **alto**.

En el desarrollo de criterios es importante:

1. Definir la cantidad de niveles necesarios para el criterio.
2. Definir el nombre del nivel.
3. Definir los valores de cada nivel.
4. Hacer una descripción detallada de cada nivel. Colocar el máximo de información que cubre ese nivel con el fin de permitir que cualquier persona entienda cada nivel del criterio y aplicarlo de manera equitativa y uniforme.

2.7.1 Criterios de impacto

El impacto es el cambio adverso en el nivel obtenido en los objetivos de negocios. Los criterios de impacto sirven para medir la cantidad de daños o costos a la organización causados por la ocurrencia de un evento de seguridad de la información. Generalmente están relacionadas con las pérdidas financieras. Deben considerar, entre otros:

- El deterioro de las operaciones;
- Incumplimiento de los plazos;
- Los daños de reputación e imagen;
- Violaciones de requisitos legales y reglamentarios;
- Gravedad y criticidad;
- El compromiso de la confidencialidad, integridad y disponibilidad;
- Otros, de acuerdo con la organización y el alcance.

Ejemplo

Si en la ocurrencia de un incendio los perjuicios fueran sólo locales, solo en una sala, el impacto puede ser clasificado como **bajo**. En la situación de que el incendio se hubiese propagado, y no hubiese sido posible controlarlo, de manera que haya destruido varias salas, equipos y documentos importantes, el impacto puede ser clasificado como **elevado**.

2.7.2 Criterios para la aceptación del riesgo

Sirven a la organización para definir su nivel o su escala de aceptación del riesgo. Dependen de las políticas, metas y objetivos de la organización, siendo definidos con la participación de la alta dirección de la organización. Debe tener en cuenta:

- Aspectos legales y reglamentarios;
- Finanzas;
- Aspectos sociales;
- Repercusión en la imagen;
- Aspectos operacionales;
- Negocios;
- Tecnologías.
- Otros, de acuerdo con la organización y la planificación de futuros negocios.

Ejemplo:

La organización señala que todo riesgo muy bajo que posee impacto bajísimo o que puedan causar pérdidas financieras por debajo de $ 10.000 se clasifica como riesgo aceptable y no serán tratados con prioridad.

Ejemplos de criterios

Tabla 5. Ejemplo de criterio de probabilidad.

Nivel	Definición
Frecuente	> 0,92
Probable	>0,65 y <=0,92
Ocasional	>0,39 y <= 0,65
Remoto	>0,15 y <=0,39
Improbable	>= 0 y <= 0,15

Tabla 6. Ejemplo de criterio de cobertura.

Valor	Definición
1	A penas en la red local
2	Restricción al sector, departamento o gerencia.
3	Afecta parte del lugar donde está activo.
4	Las consecuencias inciden sobre todo el sitio/ sucursal donde está el activo.
5	El activo tiene consecuencias sobre toda la organización.

Tabla 7. Ejemplo de criterio de nivel de riesgo.

Nivel del riesgo	Valor	Descripción
Extremo	5	De acuerdo con la organización
Altísimo	4	De acuerdo con la organización
Alto	3	De acuerdo con la organización
Medio	2	De acuerdo con la organización
Bajo	1	De acuerdo con la organización
Irrelevante	0,5	De acuerdo con la organización

Otro punto importante es la definición de los criterios (7.2. Criterios básicos). Los criterios son parte del método con el cual será realizada la gestión del riesgo. En otras palabras, los criterios son la forma y el valor (importancia) con que se valorarán los riesgos e impactos. Para identificar el mayor o menor riesgo y el más alto o más bajo impacto, es necesario definir los criterios. Criterio es una norma que sirve de base para que las cosas y las personas puedan ser comparadas y juzgadas.

La definición de los criterios de riesgo implica decidir sobre:

- La naturaleza y los tipos de consecuencias que incluyen y cómo van a ser medidos.
- La manera por la cual las probabilidades serán representadas.
- Cómo estará representado un nivel de riesgo.
- Los criterios que guiarán la decisión del tratamiento del riesgo.
- Los parámetros para definir cuando un riesgo es aceptable y/o tolerable.
- Si las combinaciones de riesgos serán tomadas en consideración.

Los criterios poden ser basados en fuentes como:

- Los objetivos acordados del proceso;
- Los criterios identificados en el pliego de condiciones;
- Las fuentes de datos;
- Criterios generalmente aceptados por la industria, como los niveles de integridad, seguridad (mejores prácticas);
- El apetito de riesgo de la organización;
- Los requisitos legales cumplidos por la organización;
- Otros medios de información técnica de los equipos específicos o aplicaciones.

Los criterios a ser adoptados deben ser determinados en común acuerdo entre el equipo de gestión del riesgo y la organización. En caso de que la organización ya cuente con criterios para otros sistemas de gestión, estos podrán ser adoptados en función de la demanda, facilitando la comprensión de los criterios para la gestión del riesgo por parte de la organización, que serán similares a los ya utilizados por otros sistemas de gestión implementados.

Tabla 8. Ejemplos de criterios de impacto.

Nivel del riesgo	Valor	Descripción
Despreciable	1	» No hay lesiones, muertes de trabajadores y/o de personas externas a la organización. Pueden ocurrir casos de primeros auxilios o tratamiento médico (sin retiro). » Sin daños o con daños menores en los equipos y/o instalaciones. » Los sistemas de las TI se quedaran fuera de servicio durante un máximo de 5 minutos.
Ligeramente perjudicial	2	» Lesiones leves en la fuerza laboral, ausencia de lesiones. » Daños leves a los equipos o instalaciones, controlables y/o de daños de bajo costo de reparación. » Los sistemas de las TI se quedaran fuera de servicio durante un máximo de 30 minutos
Perjudicial	3	» Lesiones de gravedad moderada en la fuerza laboral o en personas externas a la organización. » Lesiones leves en las personas externas a la organización. Daños severos a equipos y/o instalaciones. » Los sistemas de las TI se quedaran fuera de funcionamiento durante más de 30 minutos. Emisión de la factura por sistema alternativo. Necesidad de recuperar de copia de seguridad.
Extremadamente perjudicial	5	» Causa muerte o lesiones graves a una o más personas (la fuerza laboral y/o en personas externas a la organización). » Daños irreparables a los equipos o instalaciones (reparación lenta o imposible). » Activado sitio alternativo. Pérdida de datos e información. Clientes sin asistencia completa

Tenga en cuenta que estos ejemplos probablemente no se aplican a cualquier tipo de organización, solo a aquellas para las cuales fueron desarrollados. Sin embargo, dan una idea sobre la creación de criterios aplicados a las actividades de gestión del riesgo. En este curso se desarrollarán los criterios durante la ejecución de las actividades.

Ejercicio de refuerzo - definiendo los criterios

» ¿Qué criterios existen actualmente en su organización? Justifique.
» ¿Teniendo en cuenta el ambiente de su organización, haga una descripción de los niveles «bajos» y «altísimos» de la Tabla 8 ? Justifique.

2.7.3 Organización para la gestión del riesgo

La definición de roles y responsabilidades es un factor importante para el éxito del proceso de gestión del riesgo. Para esto debe estar formalmente definida, comunicada, documentada y aprobada por los gestores de la alta administración.

Debe quedar claro para todos los involucrados que el conjunto de estas actividades deben generar evidencias que ayuden para una aplicación adecuada de los procesos de gestión del riesgo. Por lo tanto, es importante que todas la información y datos sean documentados en el caso de una futura auditoría.

Lectura complementaria

» Sección 7 de la norma ICONTEC NTC ISO/IEC 27005.
» Sesiones 5, 6 y 7 de la norma ICONTEC NTC ISO/IEC 27002.
» Capítulo 5 del libro "El riesgo de TI" (El desarrollo del proceso de gobierno del riesgo), George Westerman y Richard Hunter: Harvard Business School Press, 2008.

Lo aprendido

» Descripción del contexto.
» Definición de alcance.
» Identificación de restricciones.
» Definición de criterios.

Capítulo

03

Identificación del riesgo

Objetivos

Comprender el proceso de identificación del riesgo e identificar los activos, amenazas y controles existentes.

Conceptos

Análisis e identificación del riesgo, amenazas y controles.

Introducción

Después de las fases de identificación del contexto y definición del alcance, la siguiente fase es el análisis/evaluación del riesgo, compuestas por dos grandes etapas de trabajo:

» Análisis del riesgo;
» Evaluación del riesgo.

En esta sesión de aprendizaje, vamos a empezar el estudio de la etapa de análisis del riesgo.

Ejercicio de nivelación - identificación del riesgo

» ¿Qué entiende por identificación del riesgo?

3.1 Proceso de análisis del riesgo de seguridad de la información

La fase de proceso de análisis del riesgo identifica y evalúa los activos, amenazas y vulnerabilidades, siendo compuesta por los siguientes pasos:

» **Identificación del riesgo:** donde son determinados los eventos que pueden causar potenciales pérdidas.
» **Análisis del riesgo:** donde se determina la probabilidad de ocurrencia de los eventos.
» **Evaluación del riesgo:** ordena los riesgos de acuerdo con los criterios de evaluación establecidos en la definición de contexto.

Después de identificar el contexto y la definición del alcance, con perfecto conocimiento de todo el ambiente, se inicia el proceso de análisis/evaluación del riesgo de seguridad de la información. Vea resaltado en la siguiente figura las actividades en el proceso de gestión del riesgo.

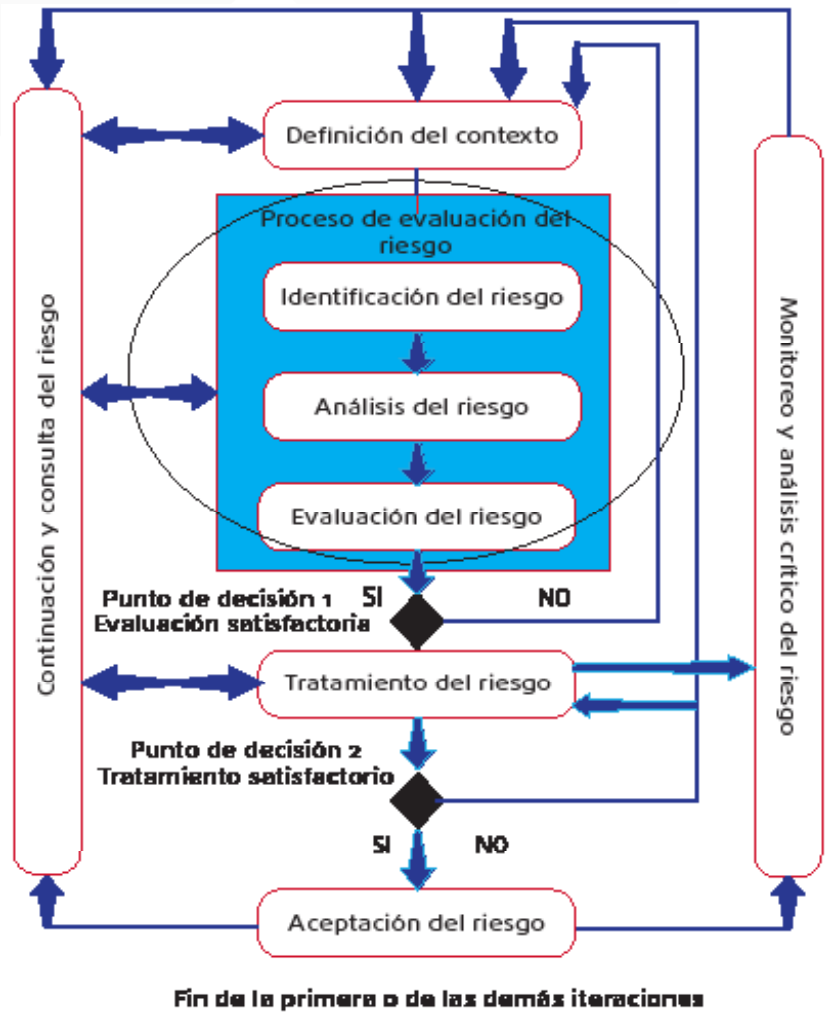


Figura 4. Posición de la fase de análisis del riesgo en el proceso de gestión del riesgo.

En este capítulo se presentarán los detalles de la identificación del riesgo.

Recomendamos su seguimiento con la lectura del ítem 8.2.1 de la norma ICONTEC NTC ISO/IEC 27005.

3.2 Identificación del riesgo

- Realizada para conocer y determinar los posibles eventos con potencial para causar pérdidas, y hacer el levantamiento de cómo esto puede suceder.
- Los resultados de esta etapa serán los datos de entrada de la etapa de estimación del riesgo.

Es importante que cualquier organización identifique a sus fuentes de riesgo, sus causas y consecuencias. El objetivo es generar una lista completa de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos.

En la fase de análisis del riesgo, el primer paso es la identificación del riesgo. Esta identificación se lleva a cabo de manera que pueda conocer y determinar los posibles eventos que tienen un potencial para causar pérdida, así como elevar la forma en que esto puede suceder. Las actividades de identificación del riesgo se muestran en la Figura 5:

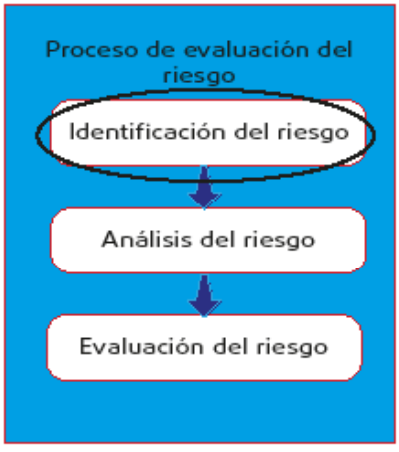


Figura 5. Identificación del riesgo en la fase de análisis del riesgo.

Las actividades de identificación del riesgo se muestran en la siguiente figura:

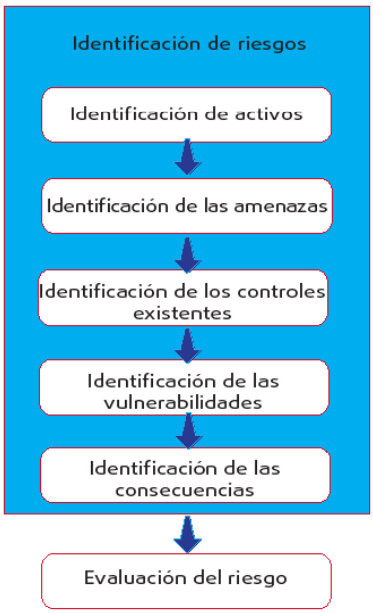


Figura 6. Actividades de la identificación del riesgo

3.3 Identificando los activos

- » Activo es cualquier elemento con valor para la organización, que necesitan protección.
  - **Entrada:** resultados de la etapa de definición del alcance.
  - **Acción:** desarrollo de la actividad de identificación de los activos.
- » Nivel de detalle que permita el suministro de información adecuada y suficiente para el análisis y evaluación del riesgo.
- » La primera información sobre cada activo es "¿quién es su responsable?"
- » Identificación de activos:
  - Activos primarios.
  - Activos de soporte y de infraestructura.

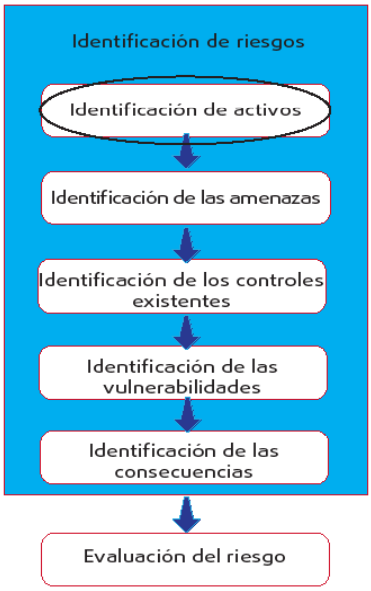


Figura 7.
Identificación
de los activos

Con la información recogida durante la fase de definición de contexto, como el alcance, lista de componentes y responsables, entre otros, se inicia la identificación de los activos.

Activo es cualquier elemento de valor para la organización, es decir, cualquier elemento tangible (como hardware) o intangible (por ejemplo, la propiedad intelectual), recurso o la habilidad que tiene valor o sea crítico para la existencia de la organización, y que por lo tanto necesita protección.

En la actividad de la identificación de los activos:

- **Entrada:** contempla los resultados de la etapa de definición del alcance.
- **Acción:** Desarrollo de la actividad de identificación de los activos. La identificación de los activos debe ser hecha a un nivel de detalle que permite el suministro de información adecuada y suficiente para el análisis y evaluación del riesgo. Como el proceso define la necesidad de varias iteraciones, el detalle puede ser profundizado en cada iteración.
- **Salida:** lista de los activos considerados sensibles para la organización y también una lista de los negocios relacionados a estos activos.

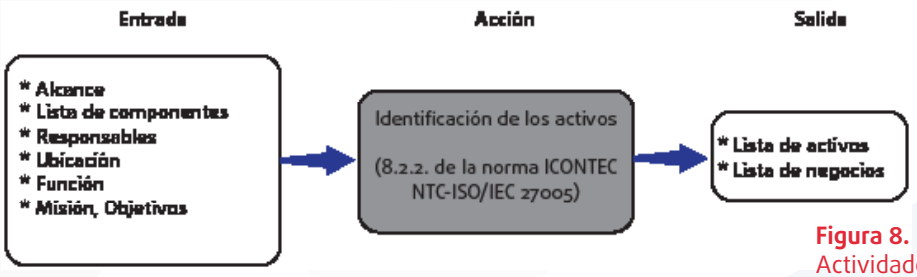


Figura 8. Actividades de la identificación de los activos

La primera información sobre cada activo es "¿quién es su responsable?". Este profesional tiene la responsabilidad sobre la producción, desarrollo, mantenimiento, utilización y seguridad del activo, tiene la mayoría de la información sobre el activo y con frecuencia será la persona más apropiada para determinar el valor del activo.

Dos tipos de activos pueden ser identificados:

» Activos primarios;
» Activos de soporte e infraestructura.

3.3.1 Identificando los activos primarios

Los activos primarios son procesos y actividades de negocios, así como la información relacionada. La mejor manera de identificar estos activos es a través de entrevistas a un grupo heterogéneo de profesionales que representan el proceso, como gestores, especialistas en los sistemas de información y usuarios. Es importante la participación de representantes de todos los niveles de la organización.

Por lo general, los activos primarios son los principales procesos e información de las actividades incluidas en el alcance de aplicación. Los activos primarios pueden ser de dos tipos:

» Procesos o subprocesos y actividades de negocio. Por ejemplo:
  - Procesos cuya interrupción (así sea parcialmente) impide a la organización continuar con su negocio;
  - Procesos que contienen procedimientos secretos o que involucran tecnología patentada.

» La información primaria puede incluir:
  - Información vital para el ejercicio de las actividades de la organización;
  - Información de carácter personal, como las definidas en las leyes nacionales sobre la privacidad.

Normalmente, la información para la identificación detallada de los activos primarios es obtenida a nivel gerencial y de la alta dirección de la organización. Estos activos serán considerados sensibles para la organización. Cabe resaltar que existirán procesos e información que no serán sensibles, pero a menudo heredan los controles para la protección de procesos e información sensible.

3.3.2 Identificando los activos de soporte e infraestructura

El Anexo B de la norma ICONTEC NTC ISO/IEC 27005 en su punto B.1.2 presenta en detalle ejemplos de los activos de soporte e infraestructura

Es importante resaltar la importancia del detalle de esta información sobre los activos. Normalmente toda la información necesaria para el equipo de análisis de riesgo no será obtenida en una primera entrevista. La realización de otras iteraciones y de entrevistas en los niveles gerenciales, técnicos y de usuarios, junto con las observaciones in situ en la organización, permitirá que sea obtenida la información suficiente para identificar los activos.

Para la actividad de identificación de los activos, el equipo de análisis tendrá como salida una lista de los activos considerados sensibles para la organización y también una lista de los negocios relacionados con estos activos.

Ejercicio de refuerzo - identificando los activos

» Nombre dos activos primarios de su organización y justifique.
» Nombre dos activos de soporte e infraestructura de su organización y justifique.

3.4 Identificando las amenazas

» Amenaza es cualquier evento que explota vulnerabilidades, con potencial de causar incidentes no deseados, que podrían resultar en daño para un sistema u organización.

» En la identificación de las amenazas son realizadas acciones para identificar dentro del alcance las amenazas existentes en la organización.

- **Entrada:** la información del historial y de incidentes pasados, de las observaciones de los responsables y usuarios de los activos, y aún de catálogos externos de amenazas.
- **Acción:** identificación de las amenazas y sus fuentes.
- **Salida:** lista de amenazas identificadas por el tipo y la fuente.

» Identificación de la fuente de la amenaza y su agente

- La amenaza tiene el potencial de comprometer los activos y las organizaciones y deben ser identificadas.
- El agente de la amenaza es una entidad con potencial para crear una amenaza, explotando o evidenciando alguna vulnerabilidad.
- El ser humano es uno de los principales y más peligrosos agentes de amenaza.
- Las amenazas pueden ser deliberadas, accidentales o de origen natural y ambiental.
- Entrevistas, visitas a sitios y listas de verificación ayudan en las acciones de identificación de amenazas.

» Es común que las amenazas afecten más de un activo.

- En estos casos, el equipo de análisis debe tener en cuenta que las amenazas pueden afectar a cada activo de manera diferente.

» Es importante recordar el cuidado con los datos y la información recibida, pues se trata de datos confidenciales y sensibles de la organización y como tal deben ser tratados.

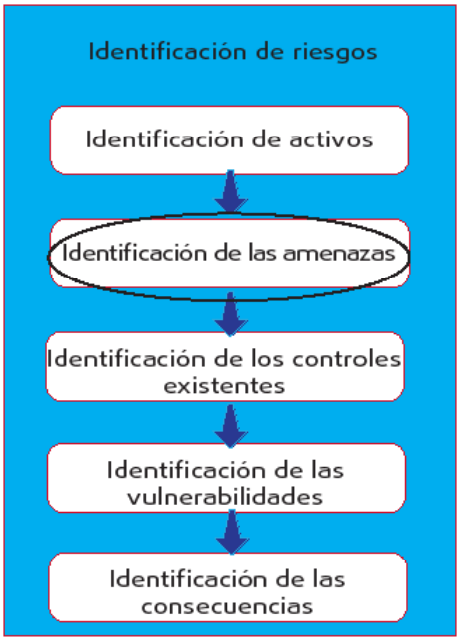


Figura 9.
Identificación de las amenazas

Como se puede notar, la amenaza es cualquier evento que explote vulnerabilidades con potencial de causar un incidente no deseado, que puede resultar en daño a un sistema u organización. En la actividad de identificación de las amenazas serán realizadas acciones para levantar e identificar, dentro del alcance establecido, las amenazas existentes en la organización.

De esta actividad de identificación de las amenazas, el equipo de análisis tendrá como:

- **Entrada:** la información de su historial, obtenidas de los incidentes ocurridos, de observaciones realizadas por los responsables y usuarios de los activos, y aún a través de información recolectada de catálogos externos de amenazas.
- **Acción:** identificación de las amenazas y sus fuentes. La fuente de amenaza está relacionada a su agente, entidad que puede causar una amenaza explotando o evidenciando alguna vulnerabilidad. Uno de los principales y más peligrosas agentes de amenaza es el ser humano.
- **Salida:** una lista de amenazas con la identificación del tipo y de la fuente de las amenazas.

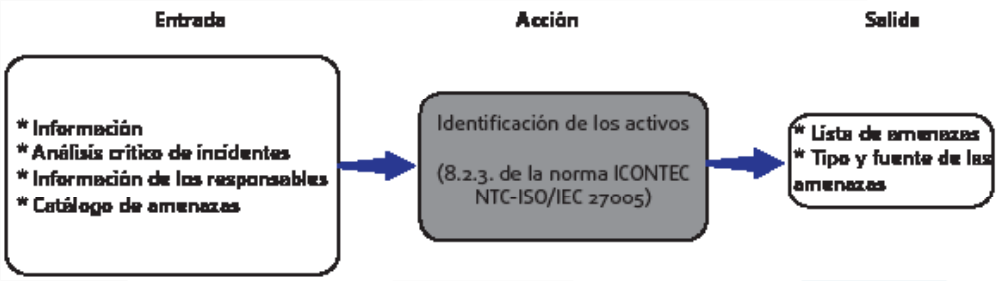


Figura 10. Actividades de la identificación de las amenazas

Las amenazas pueden ser deliberadas, accidentales o de origen natural y ambiental. El Anexo C de la norma ICONTEC NTC-ISO/IEC 27005 presenta una lista con 43 ejemplos de amenazas que abarcan múltiples tipos. Este anexo también contiene una tabla con el origen de las amenazas planteadas por el ser humano y sus motivaciones y consecuencias.

Las amenazas tienen el potencial de comprometer los activos y las organizaciones, y deben ser identificadas. Durante la actividad de identificación es necesaria la creación de un catálogo de amenazas de la organización. Este catálogo deberá contener la categoría de amenaza: si es interna (origen dentro de la organización), externa (origen fuera de la organización) o interna y externa simultáneamente.

Durante las acciones de identificación de amenazas, deben llevarse a cabo entrevistas, observaciones en el lugar y una *checklist,* con los niveles gerenciales, técnicos y también con usuarios, para tener la máxima información posible. Así puede ser obtenida la información como: datos de incidentes ocurridos, cantidad de ocurrencias, aspectos culturales y de ambiente de los activos, experiencias en ocurrencias anteriores, evaluaciones y otra información colectada en las reuniones. Toda la información debe ser registrada y compilada en un documento para su posterior utilización como prueba en caso de necesidad.

Es frecuente que algunas amenazas afecten a más de un activo. En estos casos, el equipo debe tener en cuenta que estas amenazas pueden actuar de manera diferente en cada activo, lo que los afecta de manera diferente.

Es importante recordar el cuidado con los datos y la información recibida, pues se tratan de datos confidenciales y sensibles de la organización y como tal deben ser tratados por todos los involucrados en el análisis del riesgo.

Ejercicio de refuerzo - identificando las amenazas

» Utilizando la norma, cite tres amenazas existentes en su organización y justifique su respuesta.

3.5 Identificando los controles existentes

» El control es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad.

» El objetivo es identificar en el ambiente del alcance los controles planeados para la implementación y los controles existentes, ya desplegados y en uso.

- **Entrada:** documentaciones de los controles ya existentes y los planes de implementación de control para el tratamiento del riesgo.
- **Acción:** identificación de los controles implementados y planificados.
- **Salida:** lista de todos los controles existentes y planeados, su implementación y estado de uso.

» Objetivos de la identificación de controles:

- Evitar costos y reprocesos con duplicación de controles.
- Asegurar que los controles existentes están funcionando de manera correcta y tratando el riesgo de forma deseada.

» Actividades de la identificación de controles:

- Reuniones con los responsables por la seguridad de la información.
- Entrevistas con los usuarios para identificación de los controles existentes.

- Analizar de manera crítica la documentación sobre los controles existentes.
- Realizar cuestionarios y listas de verificación.
- Hacer inspecciones físicas, visitas y observaciones en los locales.

» Controles complementares pueden ser necesarios para el tratamiento eficaz del riesgo.
» Controles ineficaces o insuficientes deben ser removidos y reemplazados.
» Controles previstos se deben evaluar si realmente serán capaces de hacer frente a los riesgos a los que se refieren al cumplimiento.

Figura 11. Fase de identificación de los controles existentes en el proceso de identificación del riesgo

El control es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad. Ejemplos de controles incluyen políticas, procedimientos, estructuras organizacionales, antivirus, parches, cerraduras, extintor de incendio y *backups*, entre otros.

En la actividad de identificación de los controles existentes, el objetivo es identificar en el ambiente del alcance los controles que están planea-

dos para implementación y los controles ya implementados y en uso corriente. En esta actividad:

- **Entrada:** documentación de los controles existentes y planes de implementación de control para el tratamiento del riesgo.
- **Acción:** identificación de los controles implementados y planificados.
- **Salida:** lista de todos los controles existentes y planeados, su implementación y status de uso.

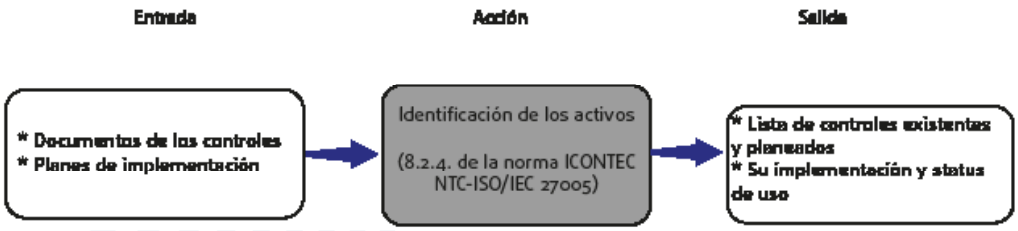


Figura 12. Identificación de los controles existentes.

Los objetivos de esta actividad son evitar re-procesos y costos adicionales para la duplicación de los controles, así como asegurar que los controles existentes estén funcionando adecuadamente, tratando eficazmente el riesgo. Una forma de realizar esta actividad es analizando informes de auditorías en el SGSI, los informes de análisis críticos de la dirección y los indicadores de la eficacia de los controles. Si esta información no está disponible, se recomienda la realización de:

- Reuniones con los responsables por la seguridad de la información;
- Entrevistas con usuarios para levantamiento de los controles existentes;
- Análisis crítico de la documentación sobre los controles existentes;
- Cuestionarios y listas de verificación;
- Inspecciones físicas y visitas a los locales.

Un control puede no cumplir plenamente y fallar en el tratamiento del riesgo. Así, controles complementarios pueden ser necesarios para el tratamiento eficaz del riesgo. Otro punto es acerca de los controles

ineficaces o insuficientes. En estos casos puede ser necesario que el control sea retirado y sustituido por otro. Estos puntos deben ser incluidos en el análisis de los controles existentes, realizado por el equipo de análisis. Controles planeados deben ser evaluados, sobre si realmente serán capaces de hacer frente a los riesgos a los que se refieren al cumplimiento.

Lectura complementaria

- Sesión 8.1, 8.2.1, 8.2.2 y 8.2.3 de la norma ICONTEC NTC ISO / IEC 27005.
- Sesión B.1 del anexo B de la norma ICONTEC NTC ISO / IEC 27005.
- Los anexos C y D de la norma ICONTEC NTC ISO / IEC 27005.

Lo aprendido

- Visión general de la identificación del riesgo.
- Metodología y actividades para identificar riesgos

Capítulo

04

Análisis del riesgo: vulnerabilidades y consecuencias

Objetivos

Identificar las vulnerabilidades y sus consecuencias.

Conceptos

Vulnerabilidades y sus consecuencias.

Introducción

El análisis del riesgo es un proceso formal para identificar las amenazas y vulnerabilidades, y a partir de esta identificación categorizar el riesgo involucrado y determinar el tratamiento apropiado.

En la secuencia de este proceso, después del conocimiento del contexto del ambiente en el que se realizará el análisis del riesgo, se deben identificar los activos, las amenazas, los controles existentes y también aquellos que necesitan ser implementados. El siguiente paso consiste en identificar las vulnerabilidades y las consecuencias que pueden ser causadas, en caso de que las vulnerabilidades sean explotadas.

Esta sesión aborda las actividades de identificación de las vulnerabilidades e identificación de las consecuencias.

Ejercicio de nivelación - vulnerabilidades y consecuencias

¿Qué entiende por vulnerabilidades y consecuencias?

4.1 Proceso de análisis del riesgo de seguridad de la información

Esta etapa de identificación del riesgo tiene cinco actividades, como se muestra a continuación:

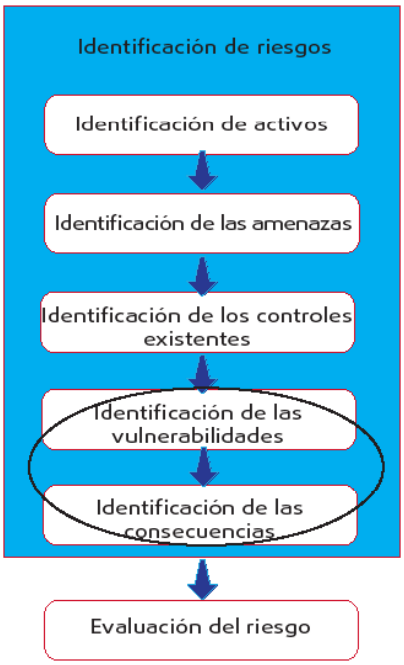


Figura 13. Identificación de las vulnerabilidades y consecuencias.

Cada actividad se debe realizar en secuencia. Estas actividades permitirán, al final de la etapa, la identificación del riesgo.

4.2 Identificando las vulnerabilidades

Durante el desarrollo de la actividad, se deben observar las siguientes áreas para la identificación de las vulnerabilidades:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión y documentación.
- Recursos humanos (incluyendo contratistas y proveedores de servicios).
- Instalaciones físicas y prediales.
- Configuración de los sistemas de información (incluidos los sistemas operacionales y aplicaciones).
- Hardware, software y equipos de comunicación.
- Dependencias de entidades externas.

Métodos proactivos:

- Las herramientas automatizadas de búsqueda e identificación de las vulnerabilidades.
- Evaluación y pruebas de seguridad.
- Prueba de invasión.
- Análisis crítica de código.

Vulnerabilidad es cualquier debilidad que pueda ser explotada y ponga en peligro la seguridad de los sistemas o información. Es una debilidad de un activo o grupo de activos que puede ser explotada para lograr una o más amenazas.

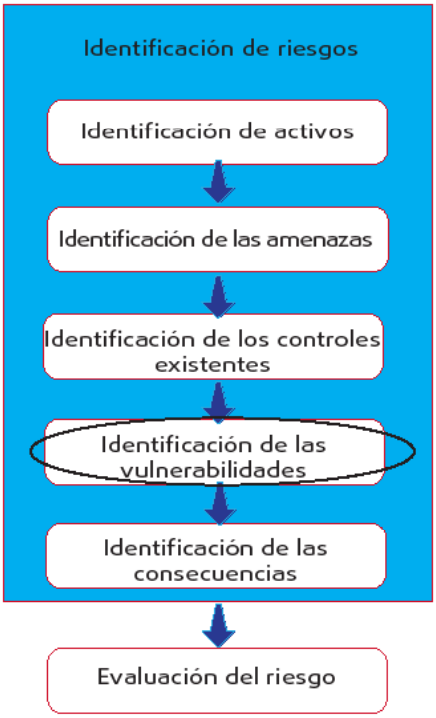
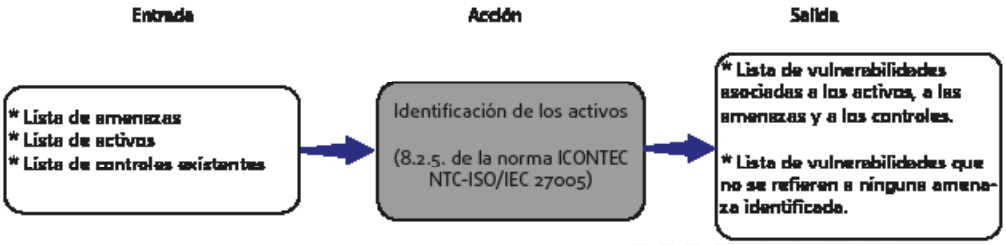


Figura 14. Identificación de las vulnerabilidades.

La actividad de la identificación de las vulnerabilidades tiene como objetivo crear una lista con las vulnerabilidades asociadas a los activos, las amenazas y los controles. En esta actividad, el equipo de análisis tendrán como:

» **Entrada:** listas de amenazas conocidas, las listas de los activos y de los controles existentes, y todas las salidas de las actividades anteriores.
» **Acción:** actividad de identificación de las vulnerabilidades que podrían ser explotadas por amenazas con la posibilidad de poner en peligro los activos.
» **Salida:** lista de escenarios de incidentes con sus consecuencias asociadas con los activos y los procesos de negocio.

Figura 15. Actividades de la identificación de las vulnerabilidades.



En la realización de la actividad de identificación de la vulnerabilidad, el equipo debe trabajar a través de dos miradas: de afuera hacia adentro y de adentro hacia afuera. Mirar desde adentro hacia afuera, es el punto de vista interno, que permite muchos privilegios. ¿Qué vulnerabilidades puedan existir o pueden ser explotados? ¿Cómo los sistemas pueden verse comprometidas por el personal interno?

En el segundo, de afuera hacia adentro, los sistemas intentarán ser comprometidos desde afuera. ¿Cuál del contenido accedido puede comprometer los activos e información de la organización? ¿Qué puede ser explorado para conferir privilegios no permitidos? Esta es la vista de un atacante que intenta irrumpir el sistema: las direcciones IP públicamente ruteables, los sistemas en la DMZ (*DeMilitarized Zone*, zona desmilitarizada), interfaces externas del *firewall,* etc. Existen diferencias notables entre estos dos tipos de evaluación de la vulnerabilidad.

El equipo de análisis debe tener en cuenta que la existencia de vulnerabilidades por sí misma no produce pérdidas, por lo tanto debe haber una amenaza. Así mismo es necesario el monitoreo de la vulnerabilidad en el caso de identificar cambios en su configuración.

Una buena práctica de esta actividad es que el equipo de análisis recorra todas las dependencias cubiertas por el alcance y realice entrevistas en su propio ambiente de trabajo con los entrevistados, lo que facilita

la formulación de cuestionamientos a partir de las observaciones en el ambiente. Es una manera de observar las vulnerabilidades y a partir de ellas identificar otras. Otra práctica que se puede utilizar es la identificación de vulnerabilidades a través del uso de métodos proactivos de ensayos, a pesar del alto costo. Entre los métodos se pueden citar:

- **Herramientas automatizadas para la búsqueda e identificación de las vulnerabilidades:** software creado para pruebas de seguridad y descubrimiento de las vulnerabilidades de forma automática, generando informes detallados de los problemas y vulnerabilidades identificados en el sistema. Las herramientas automatizadas son capaces de cruzar la información, analizarlas y comprobar las vulnerabilidades encontradas de manera eficiente. Tales herramientas han madurado, catalogando en sus bases de conocimiento la mayoría de las vulnerabilidades existentes, sin dejar de tener un costo relativamente alto.
- **Evaluación y pruebas de seguridad:** evaluación de la vulnerabilidad es un primer paso de verificación de la vulnerabilidad. Los resultados e información obtenida a través de las evaluaciones se utilizarán para la realización de las pruebas. La evaluación verifica vulnerabilidades potenciales y las pruebas de seguridad tratan de explotarlas.
- **Prueba de invasión:** tiene como objetivo comprobar la resistencia del activo en relación a los métodos de ataque conocidos.
- **Análisis crítico de código:** la identificación de las vulnerabilidades en el código fuente.

En resumen, los resultados de estos tipos de pruebas de seguridad ayudan en la identificación de las vulnerabilidades de un sistema.

El anexo D de la norma INCOTEC NTC ISO/IEC 27005 presenta una lista con varios ejemplos de vulnerabilidades, sus amenazas y métodos para la evaluación de las vulnerabilidades técnicas.

Ejercicio de refuerzo - identificando vulnerabilidades

» Nombre tres vulnerabilidades bajo la visión interna de su organización. Justifique.
» Nombre tres vulnerabilidades bajo la visión de afuera para adentro, de su organización. Justifique.

4.3 Identificación de las consecuencias

Un escenario es nada más que la descripción de una amenaza explorando una o más vulnerabilidades en un incidente de seguridad de la información.

» Ejemplos de consecuencias operacionales:

- La oportunidad perdida.
- Salud y seguridad de los profesionales involucrados.
- Tiempo de investigación y tiempo de reparación.
- Tiempo perdido de trabajo.
- Costo financiero para reparar el daño.
- Imagen y reputación.

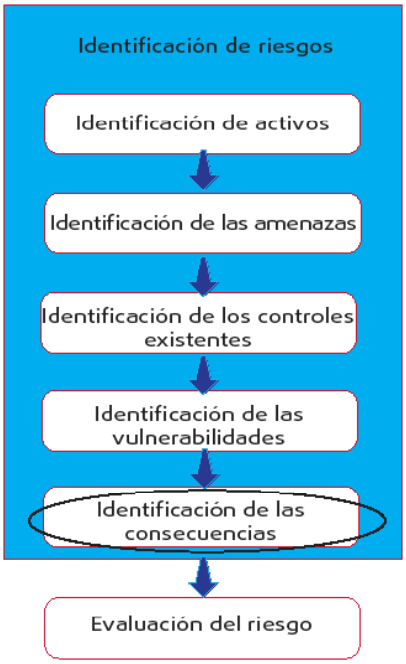
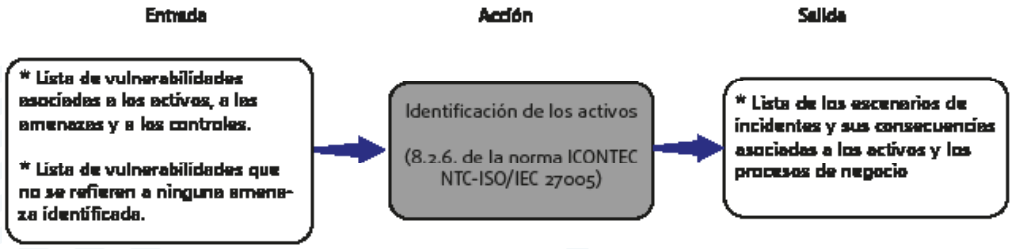


Figura 16. Identificación de las consecuencias.

Se entiende por consecuencias el resultado de un incidente o evento que puede tener un impacto en los objetivos de la organización. En esta parte del análisis del riesgo, una consecuencia puede ser, por ejemplo:

- La pérdida de eficacia en el funcionamiento operacional de los sistemas;
- La inestabilidad en el funcionamiento de sistemas;
- Condiciones adversas de operación;
- Pérdida de la oportunidad de negocios;
- Imagen y reputación afectadas;
- Violación de obligaciones reglamentarias;
- Pérdidas financieros;
- La pérdida de datos e información;
- La pérdida de vidas humanas;
- Pérdida de competitividad
- Entre muchos otros, de acuerdo con los negocios de la organización.

Figura 17. Actividades de las consecuencias.



Esta actividad tiene como objetivo identificar las consecuencias o daños para la organización que pueden ser el resultado de un escenario de incidentes, como resultado de las vulnerabilidades identificadas. La configuración de un escenario de incidentes se considera un defecto de seguridad.

Un escenario no es más que una descripción de una amenaza que explota una o más vulnerabilidades en un incidente de seguridad de la información y puede afectar a uno o más activos o apenas parte de un activo, de acuerdo con los criterios establecidos en la definición contexto. Como ejemplos de consecuencias operacionales se menciona:

- Pérdida de oportunidad;
- Salud y seguridad;
- Tiempo de investigación y tiempo de reparación;
- Tiempo de trabajo perdido;

» Costo financiero para reparar el daño;
» Imagen y reputación.

Ejercicio de refuerzo - identificando las consecuencias

» Presente una consecuencia para tres vulnerabilidades identificadas en los ejercicios de refuerzo 1. Justifique.

Lectura complementaria

» Sesión 8.2.5 y 8.2.6 de la norma INCOTEC NTC ISO/IEC 27005.
» Anexo D de la norma INCOTEC NTC ISO/IEC 27005.
» Norma Complementaria de gestión del riesgo de Seguridad de la Información y Comunicaciones - GRSIC, del DSIC/GSI/PR: http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf
» *SANS The Top Cyber Security Risks – Twenty Critical Security Controls for Effective Cyber Defense:* http://www.sans.org/
» Security Focus Vulnerabilities: http://www.securityfocus.com/
» *CERT.br Segurity Related Links:* http://www.cert.br/links/
» CASI Centro de Atendimiento a Incidentes de Seguridad - RNP: http://www.rnp.br/cais/alertas/

Lo aprendido

» Visión general de la identificación del riesgo.
» Metodología y actividades para identificar vulnerabilidades y consecuencias.

Capítulo

05

Análisis del riesgo: evaluación de las consecuencias

Objetivos

Realizar la evaluación de las consecuencias

Conceptos

Estimación del riesgo, metodologías de estimación cualitativa y cuantitativa, evaluación de las consecuencias.

Introducción

Después de la realización del proceso de identificación del riesgo, se necesita un proceso de asignación de valores a los activos, las amenazas, las vulnerabilidades y las consecuencias. Esto hace que sea posible poner los riesgos en orden de prioridad, para tratarlos de acuerdo con su urgencia o criticidad. Estos valores siguen los mismos criterios en la fase de definición de contexto.

Ejercicio de nivelación - evaluación de las consecuencias

» ¿Qué entiende por evaluación de las consecuencias?

5.1 Visión general del proceso de estimación del riesgo

» La etapa de estimación del riesgo consiste en realizar una estimación de los valores para cada uno de los elementos identificados, para ordenar el nivel de criticidad del riesgo y su posterior mitigación.
» Se puede realizar con mayor o menor detalle, en función del riesgo, del objetivo del análisis, de la información, los datos y los recursos disponibles.
» Puede ser cualitativa, cuantitativa, o la combinación de ambos.
» Desarrollado de acuerdo con los datos identificados en las actividades de las etapas anteriores.
» Estimativa de valores para cada uno de los elementos identificados para que sea posible ordenar el nivel de criticidad, del riesgo y el tratamiento posterior para la mitigación de los riesgos.

El análisis del riesgo se puede realizar con mayor o menor detalle, en función del riesgo, el objetivo del análisis, y de la información, datos y recursos disponibles. Se deben identificar los factores que afectan a la probabilidad y las consecuencias. Este análisis puede ser cualitativo, cuantitativo, o una combinación de ambos, dependiendo de las circunstancias.

La estimación del riesgo se realiza de acuerdo a los criterios del riesgo definidos por el equipo de análisis durante el inicio de los trabajos. Es importante tener en cuenta la interdependencia de los diferentes riesgos y sus fuentes.

La siguiente figura muestra la ubicación de la etapa de estimación del riesgo dentro del proceso de gestión del riesgo.

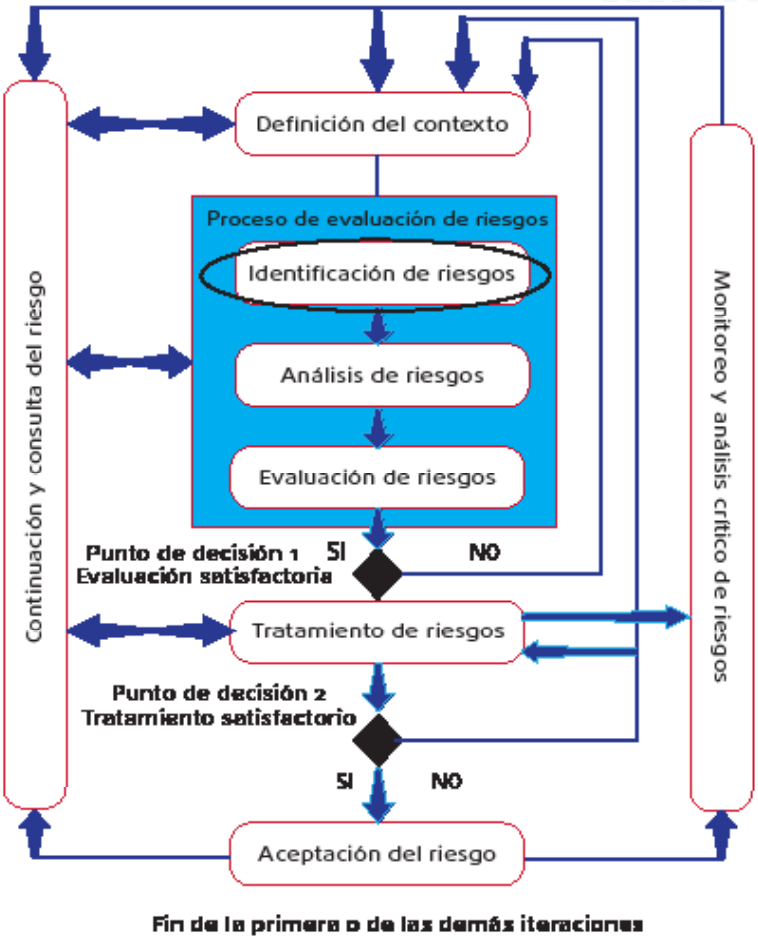


Figura 18. Etapa de estimación del riesgo.

5.2 Metodologías

Dos metodologías se pueden utilizar para el análisis del riesgo:

- Análisis cualitativo de riesgos.
- Análisis cuantitativo de riesgos.

5.2.1 Metodología de análisis cualitativo

El análisis cualitativo se basa en la evaluación, a través de atributos calificadores y descriptivos, de la intensidad de las consecuencias y la probabilidad de ocurrencia del riesgo identificado. En la metodología cualitativa no se asigna valores financieros a los activos, consecuencias o controles, sino que se utilizan escalas de atributos a través de valores descriptivos relativos.

Esta estimación es considerada demasiado subjetiva, siendo ideal para una verificación inicial de los riesgos, cuando no se dispone de suficientes datos numéricos.

Ejemplos del uso del análisis cualitativo:

Para probabilidad:

- Alta, media y baja.
- Raro, poco probable, posible, probable y casi cierto.
- Remotamente posible, ocasionalmente, a menudo, varias veces al mes.
- Improbable, probable y cierto.
- Pequeña, mediana y grande.
- Bajo, medio, alto, muy alto y elevado.
- Improbable, remota, ocasional, probable, frecuente.

Para consecuencias (impactos):

- Alta, media y baja.
- Irrelevante, Insignificante, Marginal, Crítico, Extremo y catastrófica;
- Extremo, alto, medio, bajo y despreciable;
- Grande, mediana, pequeña y banales;
- Trastornos muy graves, graves, limitados, ligeros y muy ligeros;

Los criterios anteriores son sólo ejemplos para uso educativo. El desarrollo de estos criterios debe tener en cuenta el tipo de organización, su información y datos existentes. Las escalas deberán estar construidas y adaptadas para las diferentes organizaciones y los riesgos asociados.

5.2.2 Metodología de análisis cuantitativo

En la metodología de análisis cuantitativo es utilizada una escala de valores numéricos con el objetivo de intentar calcular valores numéricos para cada uno de los componentes recolectados durante las actividades de identificación del riesgo. Un enfoque cuantitativo se adopta cuando hay un escenario que permita definir los valores financieros, aunque sea aproximado de los activos priorizados, así como los impactos. Por ejemplo, se estima que el valor real de cada activo en función del costo de reemplazo o del costo asociado a la pérdida de productividad, y otros valores de acuerdo con el tipo de organización. Esta manera de calcular puede ser empleada para el levantamiento estimado del costo de los controles y otros valores identificados en la etapa anterior. El análisis cuantitativo se debe usar datos históricos y datos precisos y auditables. Si no existe tal información, este tipo de cálculo se convierte en falso.

Ejemplos de uso de este análisis cuantitativo:

Para probabilidad:

- 50%;
- 0,2;
- 0,75

Para consecuencias (impactos):

- Valor de reposición del activo: US$ 12.000;
- Valor de mantenimiento del activo;
- Costo de implantación del control;
- Valor de la sanción por incumplimiento de contrato;
- Perjuicio por las horas de inactividad.

Complemente su aprendizaje mediante el estudio del ítem 8.3.1 de la norma ICONTEC NTC ISO/IEC 27005.

Ejercicio de refuerzo - metodologías

» Explique las diferencias entre la metodología cualitativa y la metodología cuantitativa.
» ¿Cuál es la metodología que mejor se aplica a su organización? Justifique

5.2.3 Estimación del riesgo

» Realizada después de la etapa de identificación del riesgo.
» Consta de tres actividades:
  - Evaluación de las consecuencias.
  - Evaluación de la probabilidad de incidentes.
  - Estimación del nivel del riesgo.

La etapa de estimación del riesgo se realiza poco después de la identificación del riesgo, cuando ya se ha levantado e identificado dentro del alcance acordado, los activos, las amenazas, las vulnerabilidades y sus consecuencias.

La siguiente figura ilustra, de forma didáctica, la secuencia de las actividades:

Figura 19. Actividades de la estimación del riesgo.

5.2.4 Evaluación de las consecuencias

» El propósito es evaluar el impacto en los negocios de la organización teniendo en cuenta las consecuencias de una violación de la seguridad de la información.
» El orden de los activos puede hacerse de dos maneras:
  - A través del valor de reposición del activo.
  - A través de las consecuencias para el negocio.

» La valoración de los activos y su clasificación por la criticidad son factores importantes para la determinación del impacto de un escenario de incidente.
  - El incidente puede afectar a más de un activo, debido a la interdependencia de los activos.

» Las consecuencias se pueden expresar en términos de criterios financieros, técnicos, humanos, del impacto en los negocios, entre otros criterios.
» Preparación de la lista de consecuencias evaluadas referentes a un escenario de incidente, en relación a los activos y criterios de impacto.

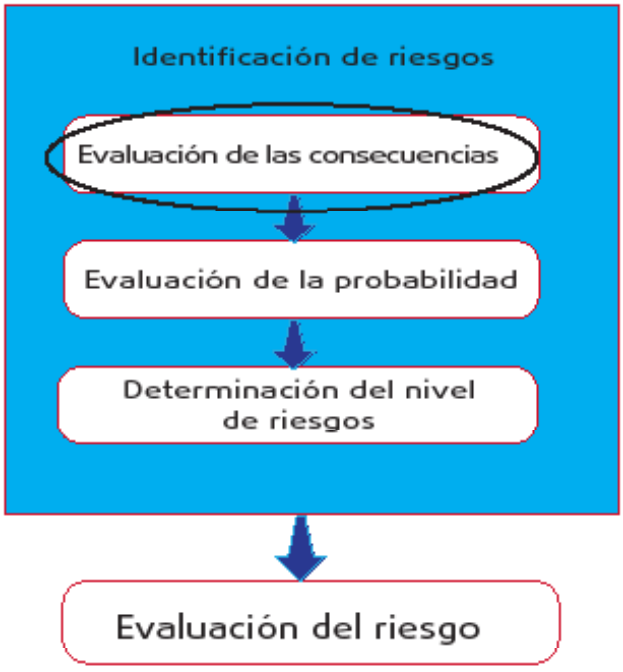
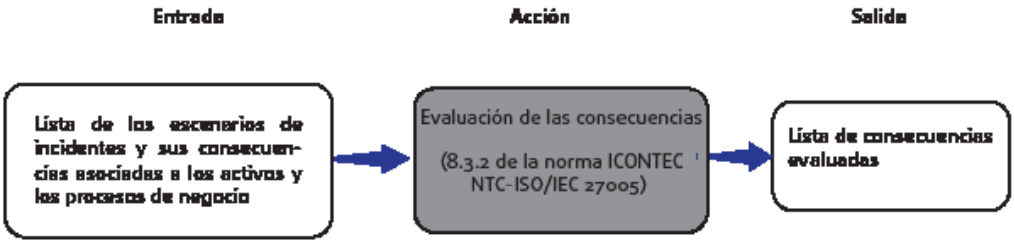


Figura 20. Evaluación de las consecuencias.

La actividad de la evaluación de las consecuencias tiene como objetivo evaluar los impactos sobre los negocios de la organización, teniendo en cuenta las consecuencias de una violación de seguridad de la información, tales como: la pérdida o degradación de la disponibilidad de los activos, la pérdida de la confidencialidad o la pérdida de integridad. Para esta evaluación, el equipo de análisis tendrá en cuenta los criterios y factores y adoptará una de las metodologías de estimativa: cualitativa o cuantitativa.

Figura 21. Actividades de la evaluación de las consecuencias.



- **Entrada:** resultados de la etapa de identificación del riesgo.
- **Acción:** exactamente el desarrollo de la actividad de evaluación de las consecuencias sobre el negocio de la organización.
- **Salida:** lista de las consecuencias relativas a un escenario de incidente, estando relacionado a los activos y criterios de impacto.

Una de las primeras acciones es el ordenamiento de los activos de acuerdo con su criticidad e importancia para el logro de los objetivos de negocio de la organización. Es posible hacer esto de dos maneras:

- **A través del valor de reposición del activo:** donde se determina el costo financiero de recuperación o reposición del activo y también del valor de la información que contenga. Por ejemplo, un servidor de correo electrónico de una organización se quemó y tiene su costo de reposición estimado en US$ 5 mil. En la metodología cualitativa el valor es alto y en la metodología cuantitativa el valor es US$ 5 mil.
- **A través de las consecuencias al negocio:** el valor se determina por el impacto de las consecuencias en los negocios. Normalmente este valor es más significativo que sólo el valor del activo. Siguiendo con el ejemplo del servidor de correo electrónico quemado del apartado anterior, se identificó que la organización trabaja con ventas de artículos deportivos hechos a mano, y sus ventas se realizan a través de e-mail, incluyendo el proceso de pago. El servidor tomó cinco días para ser restablecido y configurado, y el propietario estima que dejó de vender alrededor de US$ 20 mil por cada día parado. En la metodología cualitativa el valor es elevado y en la metodología cuantitativa el valor es de US$ 100 mil (5 días de paro x US$ 20 mil por día).

La valoración de los activos y su clasificación por la criticidad son importantes para la determinación del impacto de un escenario de incidente, pues el incidente todavía puede afectar más de un activo, debido a la interdependencia de los activos. Por lo tanto, la evaluación de las consecuencias está fuertemente relacionada con la valoración de activos. Recuerde que las consecuencias podrían ser expresadas en términos de criterios monetarios, técnicos, humanos, del impacto en los negocios u otros criterios importantes para la organización.

Lectura complementaria

» Sesión 8.3.2 de la norma ICONTEC NTC- ISO/IEC 27005.

Lo aprendido

» Metodologías cualitativa y cuantitativa.
» Cómo realizar la estimación del riesgo.
» Cómo realizar la evaluación de las consecuencias.

Capítulo

06

Análisis del riesgo: evaluación de la probabilidad

Objetivos

Realizar la evaluación de la probabilidad y determinar el nivel del riesgo

Conceptos

Probabilidad, evaluación de la probabilidad y nivel del riesgo.

Introducción

En esta etapa que es parte del proceso de análisis del riesgo, se tratan las actividades de identificación de las probabilidades de ocurrencia y la determinación del nivel del riesgo. Estas dos actividades comprenderán la finalización del proceso de análisis del riesgo.

Ejercicio de nivelación - evaluación de la probabilidad

» ¿Qué es probabilidad en un proceso de gestión del riesgo?

6.1 Visión general del proceso de evaluación del riesgo

Como fue detallado con anterioridad, el proceso de evaluación del riesgo consta de tres actividades básicas. En esta sesión se abordará dos, como se muestra a continuación:

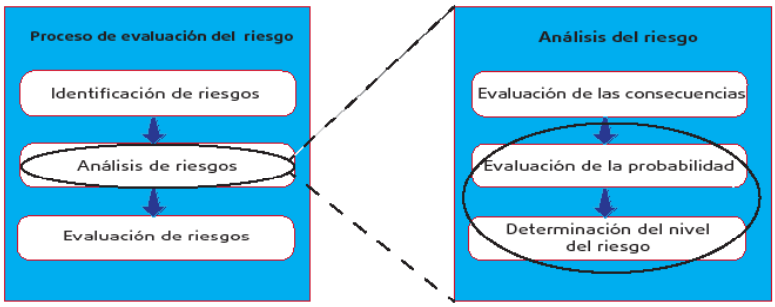


Figura 22. Estimativa y evaluación del riesgo.

6.2 Evaluación de la probabilidad de ocurrencia de incidentes

- Evaluación de la probabilidad de ocurrencia de incidentes en cada escenario y sus impactos.
- Para la estimación de la probabilidad será necesario:
  - Estudio del histórico de ocurrencias de incidentes de seguridad.
  - Informe de frecuencia de ocurrencia de las amenazas y de los niveles de posibilidad de explotación de las vulnerabilidades identificadas.
- Para la estimativa de la probabilidad el equipo de análisis debe considerar:
  - La experiencia pasada y las estadísticas históricas aplicables a la amenaza específica.
  - Las vulnerabilidades, tanto por separado como en conjunto.
  - Los controles existentes y la eficiencia y eficacia con que reduzcan las vulnerabilidades.
- Metodologías de análisis:
  - Cualitativa
  - Cuantitativa

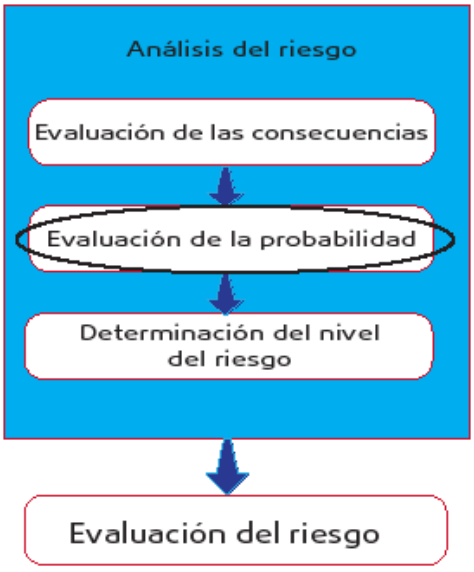


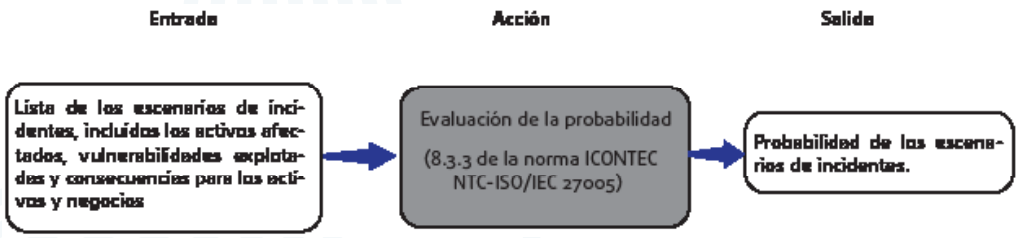
Figura 23. Evaluación de la probabilidad.

Tras la identificación de los escenarios de incidentes y la evaluación de las consecuencias, es necesario realizar la evaluación de la probabilidad del riesgo en cada escenario y los impactos correspondientes. En esta actividad es importante utilizar el historial de ocurrencias de incidentes de seguridad.

En la actividad de la evaluación de la probabilidad de incidentes:

- **Entrada:** listas de escenarios de incidentes identificados como relevantes en la actividad de evaluación de las consecuencias.
- **Acción:** evaluación de la probabilidad de ocurrencia de incidentes de seguridad.
- **Salida:** probabilidad de los escenarios de incidentes en el método cuantitativo o cualitativo.

Figura 24. Evaluación de la probabilidad de los incidentes.



Para esta evaluación se utilizan metodologías para el análisis cuantitativo y cualitativo. Para que el equipo estime la probabilidad es necesario realizar el estudio del historial de ocurrencias, la frecuencia de ocurrencia de las amenazas y de la facilidad con la que las vulnerabilidades pueden ser explotadas. Como ejemplo, consideremos las siguientes declaraciones en las entrevistas:

- **Histórico:** "consta que hace cerca de tres años ocurrió una indisponibilidad del servidor por falla de hardware."
- **Frecuencia:** "Se encontró fallos de software y 'bloqueo' del servidor del correo electrónico, pero luego vuelve a funcionar el servidor. Esto ha ocurrido en cinco ocasiones en los últimos dos meses."
- **Facilidad:** "el servidor de correo electrónico ha estado en la sala del almacén. Esto hace que sea más fácil para despachar peticiones. El personal accede directamente al servidor de correo electrónico. Esto no es un entorno cerrado, hay cerca de nueve personas que trabajan allí."

En la estimativa de la probabilidad, el equipo de análisis debe tener en cuenta la experiencia pasada y las estadísticas históricas aplicables a la determinada amenaza.

Fuentes de amenazas intencionales:

- Motivación para explotar, conflictos con superiores y la insatisfacción laboral.
- Habilidades y conocimientos: ciertas vulnerabilidades sólo puede ser explotadas si el atacante tiene elevado conocimiento técnico, para explotar otras vulnerabilidades simplemente desconectando la alimentación.
- Conocimiento de la vulnerabilidad, porque no todo el mundo puede percibir la existencia de la vulnerabilidad, aunque algunos ya saben dónde se almacena la contraseña.
- Poder de atracción de los activos: para un atacante motivado para causar gran daño, un servidor de e-mail no es suficiente, sin embargo, puede ser suficiente para otro atacante con el objetivo de provocar pequeños problemas, como sacar el servidor del aire.

Para las fuentes de amenazas accidentales:

- Proximidad a lugares insalubres y que pueden dañar los equipos;
- Eventos climáticos tales como tormentas, inundaciones y tormentas de viento;
- Factores facilitadores, que permiten que un error humano accidental (como la manipulación por personas no capacitadas técnicamente) impliquen errores (por ejemplo, red eléctrica inestable).

Las vulnerabilidades se deben analizar en forma individual y en conjunto, así como los controles existentes y la eficiencia y eficacia con que se están reduciendo las vulnerabilidades.

Por lo tanto, al analizar un determinado activo de acuerdo con los factores mencionados, el equipo de análisis puede tener el siguiente resultado, basados en las dos metodologías de estimación:

- **Cualitativa:** alta probabilidad de ocurrir una falla de disponibilidad, pues el equipo está situado en un área de alta humedad;
- **Cuantitativo:** probabilidad de 75% de ocurrir un fallo de disponibilidad, pues el equipo está situado en una zona con alta humedad.

Ejercicio de refuerzo - evaluación de la probabilidad

» ¿Cómo evaluará la probabilidad en su organización? Explique.

Determinación del nivel del riesgo

La determinación del nivel del riesgo es una actividad en la cual el equipo de análisis va a medir el nivel del riesgo con el uso de los resultados obtenidos en las etapas anteriores. En esta actividad se confieren valores a la probabilidad y consecuencias del riesgo. Esta actividad es el inicio de la construcción de la tabla de análisis del riesgo.

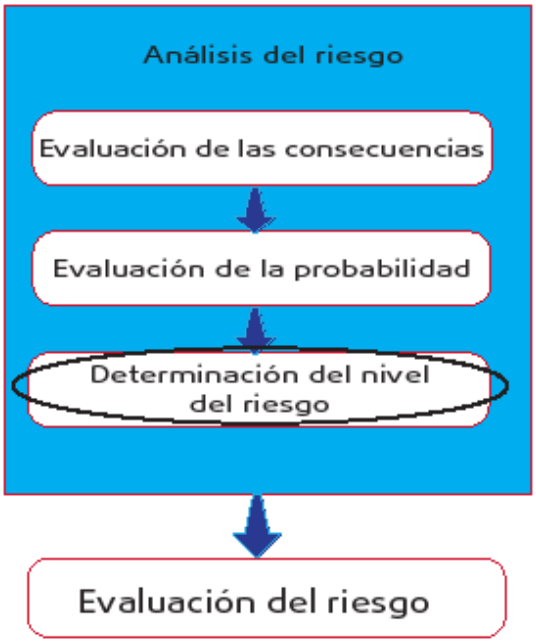


Figura 25. Determinación del nivel del riesgo.

La determinación del nivel del riesgo es una actividad en la cual el equipo de análisis medirá el nivel del riesgo con el uso de los resultados obtenidos en las etapas anteriores. En esta actividad se darán valores para la probabilidad y consecuencias del riesgo.

En esta actividad de determinación del nivel del riesgo:

- **Entrada:** son las listas de escenarios de incidentes identificados con sus consecuencias y probabilidades en la actividad de evaluación de la probabilidad.
- **Acción:** determinación del nivel del riesgo para todos los incidentes considerados.
- **Salida:** una lista de riesgos con niveles de valores.

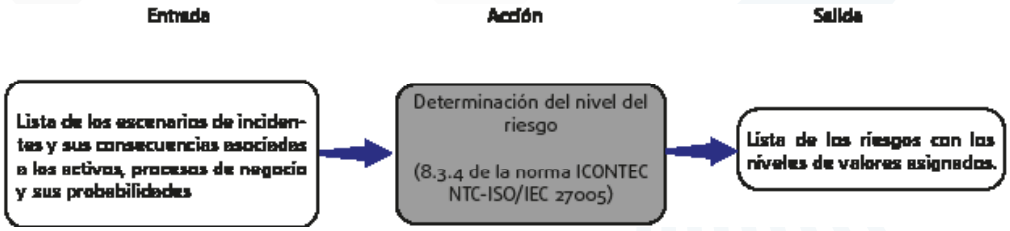


Figura 26. Determinación del nivel del riesgo.

Esta actividad es el inicio de la construcción de la tabla para analizar los riesgos. El ítem E.2 del anexo E de la norma ICONTEC NTC ISO/IEC 27005 detalla los métodos existentes para esta estimación. La elección del método ideal es resultado del tipo de organización y de su estructura para la gestión del riesgo.

El equipo de análisis debe elegir el método que mejor se adapte a las necesidades del negocio de la organización y que sea de fácil comprensión por sus miembros.

Para pensar

Lea cuidadosamente el Anexo E. Después de la lectura, elija el método que piensa que encajaría mejor en su organización. Después de elegir empiece a trabajar con este modelo.

Lectura complementaria

» Sesión 8.3.3 de la norma ICONTEC NTC ISO/IEC 27005.
» Sesión 8.3.4 de la norma ICONTEC NTC ISO/IEC 27005.
» Anexo E de la norma ICONTEC NTC ISO/IEC 27005.

Lo aprendido

» Concepto de probabilidad y estimación del riesgo.
» Cálculo de la probabilidad de ocurrencia del riesgo.

Capítulo

07

Evaluación del riesgo

Objetivos

Conceptualizar, definir y ejecutar la evaluación del riesgo.

Conceptos

Evaluación del riesgo.

Introducción

Con los resultados obtenidos en las fases anteriores, el equipo de análisis ya tiene suficientes datos para iniciar el proceso de evaluación del riesgo, fase responsable por ordenar los riesgos por la prioridad de acuerdo con los criterios de evaluación del riesgo definidos.

Este capítulo debe ser realizado con consulta a la norma ICONTEC NTC-ISO/IEC 27005.

Ejercicio de nivelación - evaluación del riesgo

» ¿Cuál es la información que usted ya tiene para iniciar la evaluación del riesgo? Explique.

7.1 Proceso de evaluación del riesgo de seguridad de la información

El objetivo del proceso de evaluación del riesgo es ayudar en las decisiones sobre la base de los resultados del análisis del riesgo. Esta etapa de la gestión del riesgo tiene por objetivo comparar los niveles de riesgos identificados en la fase anterior con los criterios de evaluación y aceptación del riesgo. Estos criterios son definidos durante la definición del contexto y deben estar alineados con los objetivos de la organización.

Fase de evaluación del riesgo:

» **Entrada:** lista de los riesgos con los niveles de valores y criterios para la evaluación del riesgo.

» **Acción:** comparación del nivel del riesgo con los criterios de evaluación.
» **Salida:** lista de riesgos ordenados por priorización, de acuerdo a los criterios de evaluación del riesgo.

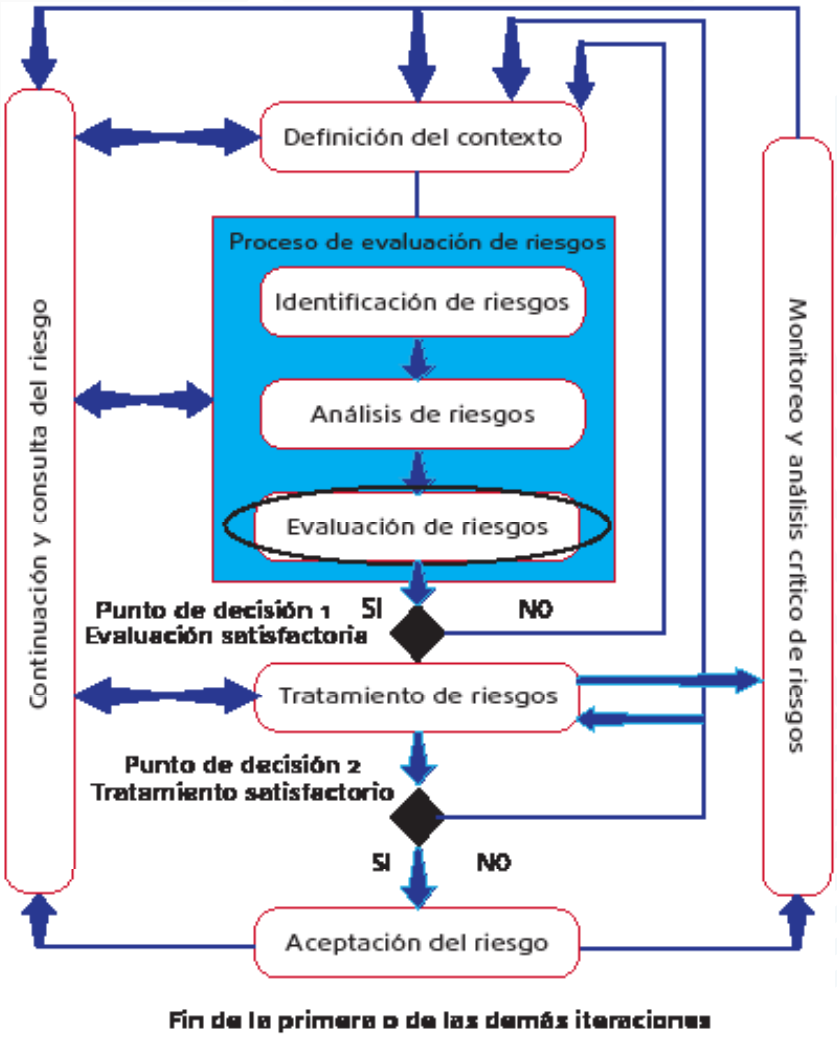


Figura 27. Evaluación del riesgo.

7.2 Evaluación del riesgo de seguridad de la información

Comparación de los riesgos estimados con los criterios de evaluación definidos en fase de contexto.

» La organización debe tomar las decisiones de esta fase en función del nivel del riesgo aceptable.

Es importante que la organización considere también:

» Las propiedades de seguridad de la información (CIDA):
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.
  - Autenticidad.

» La importancia de los procesos de negocios o de la actividad soportada por un activo o grupo de activos.

» La unión de riesgos pequeños y medianos que puede resultar en un riesgo total significativo, para tratarlos de esta manera.

» La consideración a los requisitos contractuales, reglamentarios y legales.
  - Actividad a ser concluida en conjunto con la organización, dado que sólo ella tiene la visión completa de los objetivos estratégicos de su negocio.

En esta fase los equipos de análisis en conjunto con la organización deben comparar los riesgos estimados (métodos en el Anexo E de la norma) con los criterios de evaluación establecidos durante la fase de contexto. La organización debe tomar decisiones en esta fase en función del nivel del riesgo aceptable. Sin embargo, factores como consecuencias, probabilidad y confianza deben ser considerados para una mejor toma de decisión.

Durante esta evaluación es importante que la organización considere:

» Las propiedades de seguridad de la información (Confidencialidad, Integridad, Disponibilidad, Autenticidad, CIDA): si una de estas propiedades no es importante para la organización, ella podrá considerar como de bajo valor los riesgos que causan vulnerabilidades relacionadas a esta propiedad, y así encuádralos como riesgos aceptables.

» La importancia de los procesos de negocio o de la actividad soportada por determinado activo o conjunto de activos: si un proceso o actividad es valorada por la organización como de baja importancia, los riesgos asociados a él deben ser también

menos tenidos en cuenta que los riesgos que causan impactos en procesos o actividades más importantes.

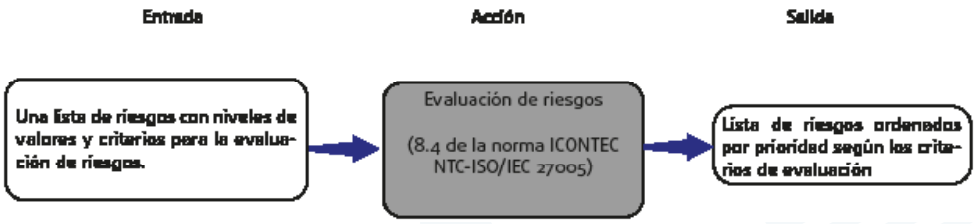
Ejercicio de refuerzo - evaluación del riesgo

» Explique la importancia de las propiedades de la seguridad de la información para su organización.

Otro punto importante a tener en cuenta durante la evaluación del riesgo es la suma de una serie de riesgos que se consideran pequeños o medianos para, a través de esta agregación, convertirlos en un riesgo total mucho más significativo, y así tratarlos adecuadamente.

En esta fase es importante que los equipos de análisis evalúen los requisitos contractuales, reglamentarios y legales. Esta actividad debe ser realizada en conjunto con la organización, porque sólo ella tiene la visión completa de sus objetivos estratégicos de negocio.

Figura 28. Fase de evaluación del riesgo.



Lectura complementaria

» Sesión 8.4 de la norma ICONTEC NTC ISO/IEC 27005.
» Anexo E de la norma ICONTEC NTC ISO/IEC 27005.
» Ítem 5.4.4 de la norma ICONTEC NTC ISO 31000.

Lo aprendido

» Comprender el proceso de evaluación del riesgo.
» Llevar a cabo una evaluación del riesgo.

Capítulo

08

Tratamiento y aceptación del riesgo

Objetivos

Conceptualizar y definir el tratamiento del riesgo, desarrollar y poner en práctica el plan de tratamiento del riesgo, entender y aplicar las formas de tratamiento del riesgo definir el riesgo aceptable y el riesgo residual, y ejecutar la aceptación del riesgo.

Conceptos

Tratamiento y aceptación del riesgo, riesgo residual y riesgo aceptable.

Introducción

La labor realizada por el equipo de análisis hasta este punto era básicamente la recopilación de información, evaluación del riesgo y ordenamiento de los riesgos por prioridad. Pero, ¿cómo hacer frente a estos riesgos? ¿Cómo seleccionar los controles necesarios? Estas dudas serán resueltas en la fase de tratamiento del riesgo de seguridad de la información.

En este capítulo debe ser realizado con consulta a la norma NTC ISO/IEC 27005.

Ejercicio de nivelación - tratamiento y aceptación del riesgo

» ¿Cómo son ejecutados el tratamiento y la aceptación del riesgo en su organización? Explique.

8.1 Visión general del proceso de tratamiento del riesgo

Fase posterior a las fases de definición del contexto, análisis del riesgo y evaluación del riesgo. Al final de estas tres fases, el equipo hace un análisis crítico de los resultados y de la situación de los trabajos realizados. Si la evaluación es considerada satisfactoria, el equipo continúa con sus trabajos e inicia la fase siguiente, el tratamiento del riesgo.

La fase de tratamiento del riesgo se realiza después de las fases de definición del contexto, el análisis del riesgo y la evaluación del riesgo. Al final de estas tres fases, el equipo hace un análisis crítico de los resultados y verifica la situación de los trabajos realizados.

En caso que esta evaluación sea considerada insatisfactoria o incompleta, el equipo vuelve al trabajo a partir de la definición del contexto, tratando de resolver las dudas que hayan podido surgir, o rehacer el trabajo desde el principio, buscando una mayor claridad. Si la evaluación es considerada satisfactoria, el equipo continúa su trabajo y realiza la siguiente fase, el tratamiento del riesgo. La siguiente figura muestra el posicionamiento de esta fase:

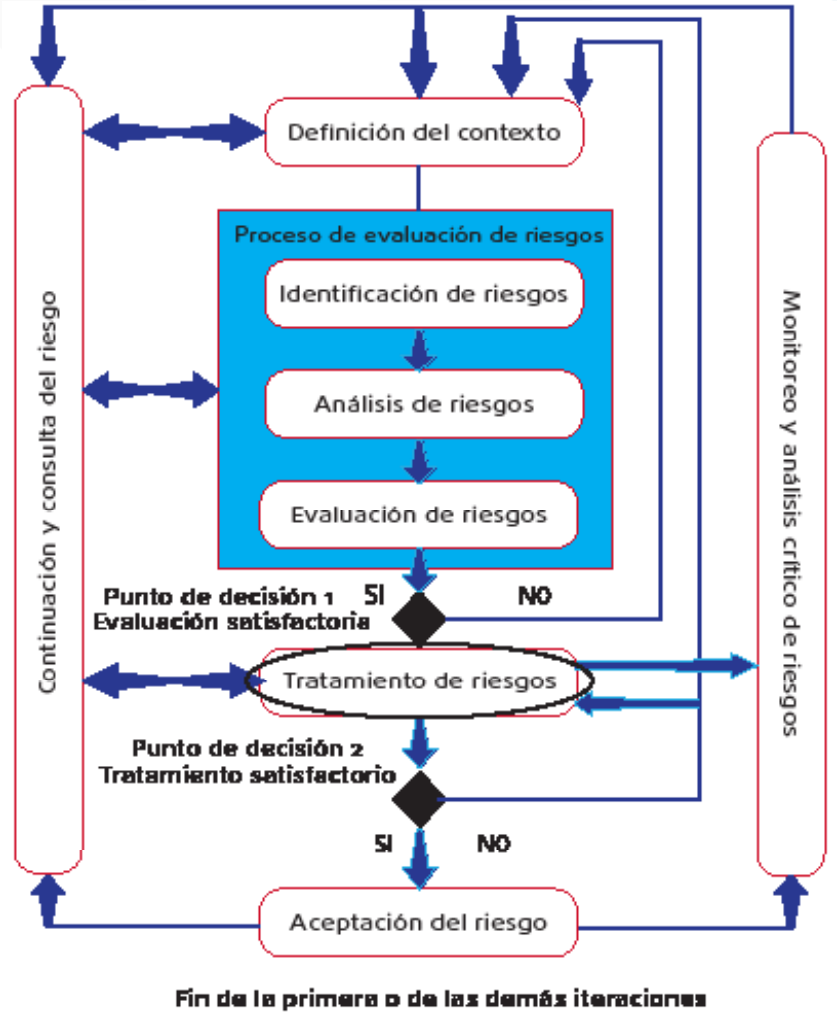
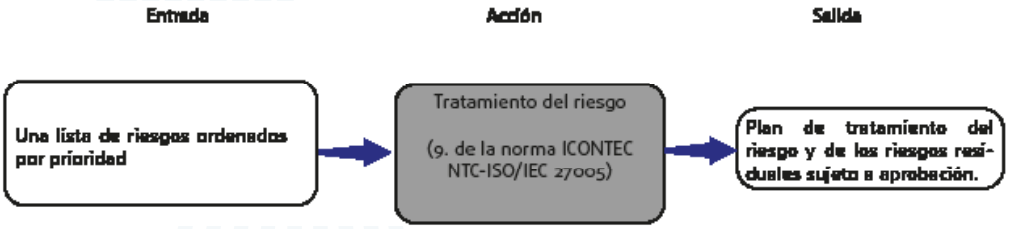


Figura 29. Tratamiento del riesgo.

En el tratamiento del riesgo el equipo de análisis tendrá como:

- **Entrada:** lista de riesgos ordenados por prioridad, asociados a los escenarios de incidentes.
- **Acción:** identificación de los controles para reducir, retener, evitar o transferir los riesgos y la definición del plan de tratamiento.
- **Salida:** plan de tratamiento del riesgo y de los riesgos residuales. Este plan estará sujeto a la aprobación de los gestores de la organización.

Figura 30. Tratamiento del riesgo.



La siguiente figura muestra las actividades del proceso de tratamiento del riesgo.

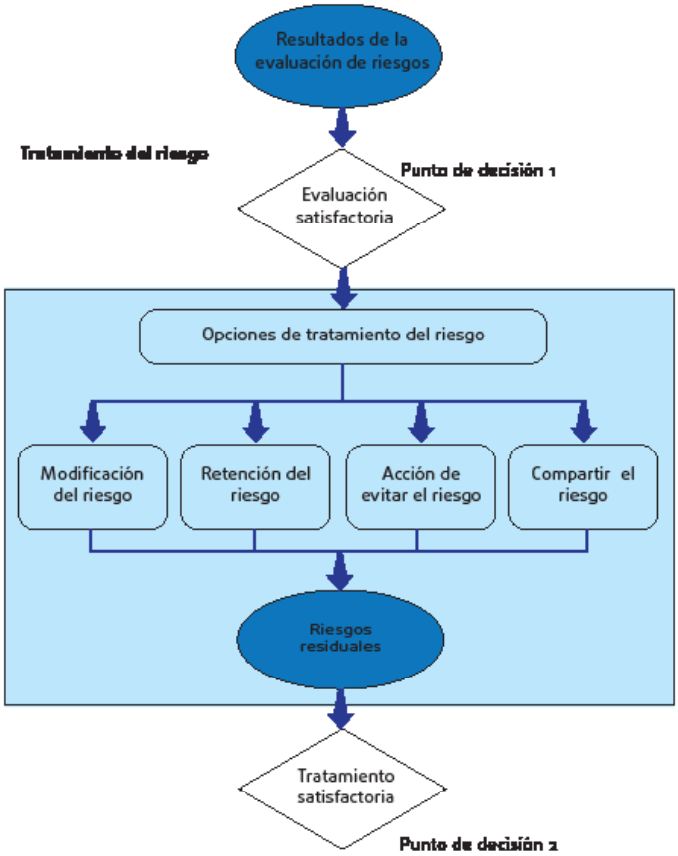


Figura 31. Actividades del tratamiento del riesgo.

8.2 Tratamiento del riesgo

El tratamiento del riesgo se utiliza para responder a los riesgos identificados. Las elecciones y decisiones deben tener en cuenta:

- La evaluación del tratamiento del riesgo propuesto ya realizado.
- La viabilidad técnica y financiera.
- La eficacia de los controles.
- La eficacia del tratamiento.
- Decisión sobre si los niveles del riesgo residual son tolerables.
- Las características del negocio de la organización.

La fase de tratamiento del riesgo tiene cuatro opciones, que no son mutuamente excluyentes:

- Modificación del riesgo.
- Retención del riesgo.
- Acción para evitar el riesgo.
- Compartir el riesgo.

Para la decisión de remoción de los controles, es imprescindible que el equipo tenga la idea de la interdependencia de los activos y sus controles, para que esta decisión no cause la reducción de la seguridad como un todo.

El equipo debe elaborar un plan de tratamiento.

El plan aborda los índices de reducción del riesgo con la implementación de cada control, permitiendo a los gestores una decisión basada en indicadores y metas bien definidos.

Una forma de identificar los controles es seguir la norma NTC-ISO/IEC 27002.

El tratamiento del riesgo se utiliza para responder a los riesgos identificados. Hay diferentes opciones para tratar y responder al riesgo. Las elecciones y decisiones tomadas por el equipo de análisis, en conjunto con la dirección de la organización, deben tener en cuenta:

- La evaluación del tratamiento del riesgo propuesto ya realizado.
- La viabilidad técnica y financiera, es decir, los costos de implementación del control.
- La eficacia de los controles.
- La eficacia del tratamiento.
- Decisión si los niveles del riesgo residual son tolerables.
- Las características del negocio de la organización (viabilidad económica).

Después de este análisis sobre los controles necesarios para el tratamiento del riesgo, el equipo debe seleccionar la mejor opción para reducir el riesgo a un nivel aceptable o hasta un mínimo posible. La fase de tratamiento del riesgo tiene cuatro opciones que no son mutuamente excluyentes, es decir, que pueden ser combinadas entre sí:

- Modificación del riesgo.
- Retención del riesgo.
- Acción para evitar el riesgo.
- Compartir el riesgo.

Estas opciones son definidas por el equipo de análisis teniendo en cuenta todo lo que ha sido identificado en el proceso de análisis. En la definición de los controles necesarios, el equipo va desarrollando una visión general de todos los controles, tanto los identificados como necesarios cuanto los identificados como implementados. De esta manera permite el levantamiento de los controles redundantes e innecesarios, posibles de remoción.

Para tomar la decisión de remover los controles, es imprescindible que el equipo tenga una noción precisa de la interdependencia de los activos y de sus controles, para que la decisión no provoque la reducción de la seguridad como un todo. Durante esta fase, todas las restricciones levantadas en la definición del contexto deberán ser tenidas en consideración durante el proceso de tratamiento del riesgo.

Después de la decisión del tratamiento necesario, el equipo deberá armar un plan. El plan es un ordenamiento de los riesgos y controles a ser implementados en función de su grado de impacto en los negocios. En principio los riesgos de mayor impacto deben ser los primeros en ser tratado.

Sin embargo, debido al costo y la demora de la implementación de los controles de los riesgos más críticos, puede ser más interesante empezar por los controles de costo más bajos y más rápidos de ser implementados. Esto puede ser una buena opción en caso se quiera presentar resultados rápidos para apoyar una política de concientización y capacitación en seguridad de la información. Recuerde, sin embargo, que esto no significa olvidar los otros controles.

Una forma de identificar los controles es seguir la norma NTC ISO/IEC 27002.

La aprobación del plan de tratamiento corresponde a los gestores de la organización. Por lo tanto, es extremadamente importante que el plan aborde los índices de reducción del riesgo. La implantación de cada control permitirá a los gestores una decisión basada en indicadores y metas bien definidas.

Seleccionar la opción más adecuada de tratamiento del riesgo consiste en equilibrar los costos y los esfuerzos que se requieren para implementar un lado y del otro, los beneficios recurrentes, teniendo en cuenta los requisitos legales, reglamentarios o de otro tipo. Es importante que el plan identifique claramente el orden de prioridad en que cada tratamiento y control que deba ser implementado.

8.3 Riesgos residuales

Una vez que el equipo definió el plan de tratamiento, es necesario determinar los riesgos residuales que permanecen después de la implementación de los controles para evitar, transferir o mitigar los riesgos. Esto es, después de la implementación de un determinado control, es posible que no sea suficiente para mitigar totalmente un riesgo. La diferencia, es decir, la posibilidad que queda de ocurrencia del riesgo, después de la implementación del control para mitigarlo, caracteriza el riesgo residual. En otras palabras, son los riesgos restantes después de tomar medidas para evitarlos, transferirlos o mitigarlos.

El riesgo residual debe ser identificado y tratado a través de la implementación de los controles. En el caso en que determinado riesgo esté por encima del nivel de aceptación del riesgo establecido por la organización, puede ser necesario realizar una nueva iteración. También se incluyen como riesgos residuales aquellos con poca importancia, o que deben ser aceptados.

8.4 Modificación del riesgo

La forma de tratamiento del riesgo llamada modificación o mitigación del riesgo es la acción para implementar controles que buscan reducir los riesgos a un nivel aceptable por la organización. La elección de estos controles debe tener en cuenta los criterios de la organización para la aceptación del riesgo, tales como: requisitos jurídicos, reglamentarios, contractuales, culturales y ambientales y aspectos técnicos, incluidos

los costos y los plazos para la implementación de controles. En general, la elección de estos controles debe proporcionar, cuando son aplicados e implementados, uno o más tipos de protección:

- **Corrección:** actividades mediante la implementación de control realizadas para corregir cualquier anormalidad;
- **Eliminación:** aplicación de controles con el fin de excluir posibles errores y vulnerabilidades o fuentes de errores y vulnerabilidades, pero sin eliminar el riesgo, sólo reduciéndolo;
- **Prevención:** implementación de controles para prevenir y detener la explotación de cualquier vulnerabilidad;
- **Minimizar el impacto:** implementación de controles que buscan reducir o limitar los daños cuando se produce un incidente de seguridad;
- **Disuasión:** acción, actividad o medida de control organizado y llevado a cabo con el fin de hacer cambiar de opinión, intención o idea;
- **Detección:** actividades de implementación de controles realizadas con el fin de descubrir errores o anomalías;
- **Recuperación:** actividad de implementación de control realizada a fin de volver a la situación normal;
- **Monitoreo:** actividad de la aplicación de controles para acompañar y observar desviaciones y observa las señales de advertencia de vulnerabilidades, amenazas y riesgos, todo con el propósito de hacer los arreglos por adelantado;
- **Conciencia:** aplicación de controles y las actividades de enseñanza que tienen como objetivo orientar sobre la seguridad de la información, de modo que todos los usuarios sepan aplicar los conocimientos relacionados en su rutina personal y profesional.

En la definición y selección de los controles, el equipo de análisis debe tener en cuenta los costos de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles relativos al valor del activo a proteger. Esto permitirá evitar la elección de controles cuyos costos serán más altos que el costo del activo o de servicios generados por él.

Anexo F de la norma ISO/IEC 27005 presenta en detalles las restricciones que afectan a la reducción del riesgo.

El equipo deberá estar atento a la "falsa sensación de seguridad." La implementación de algunos controles puede dar una falsa sensación de seguridad, dado que, por su complejidad o falta de conocimiento del usuario, pueden existir alternativas para eludir estos controles, esquivando a los esfuerzos de los administradores para proteger la seguridad

de la información. En las acciones de reducción del riesgo también se deben considerar las restricciones existentes en la organización, lo que afectará a la elección y la implementación de los controles.

8.5 Retención del riesgo

La retención del riesgo es la aceptación del riesgo de una pérdida, es decir, "correr el riesgo", incluyendo los riesgos que aún no han sido identificados. Debe ser hecho de acuerdo con los criterios de aceptación del riesgo definidos por la organización, en este caso no siendo necesaria la implementación de los controles. Es una decisión consciente de la alta dirección y debe estar bien fundamentada y registrada. Es importante que se cree un registro de los riesgos asumidos, sobre la base de su aceptación y la relación de los responsables por su aprobación.

8.6 Acción para evitar el riesgo

Cuando el equipo de análisis identifica riesgos extremadamente altos, y los costos para la implementación de controles son mayores que los beneficios del propio servicio o negocio, es posible decidir que el riesgo debe ser 100% evitado. Esto se hace mediante la eliminación de la actividad o proceso, a través de cambios en la forma de ocurrencia de la actividad o proceso capaz de producir el riesgo. Otra forma de evitar el riesgo es mediante la eliminación de la fuente de riesgo. Algunos cambios pueden ser necesarios, después de lo cual se debe realizar la nueva iteración de análisis del riesgo.

8.7 Compartir el riesgo

Compartir el riesgo involucra la transferencia de los riesgos con una entidad externa. Una forma de compartir el riesgo es el uso de seguros que cubran las consecuencias de la ocurrencia de un incidente de seguridad de la información.

Otra forma de transferencia es el uso de servicios de socios (outsourcing) para la gestión de eventos de seguridad de la información. Aunque se pueden transferir las operaciones con cierto riesgo, la responsabilidad legal por las consecuencias no será transferida.

Ejercicio de refuerzo - tratamiento del riesgo

» ¿Cuál es la forma de tratamiento que usted utilizaría para tratar el riesgo «robo/pérdida de documentos clasificados»? Justifique.
» ¿Cuál es la forma de tratamiento que usted utilizaría para tratar el riesgo «faltas constantes de electricidad»? Justifique.
» Explique la diferencia entre riesgo aceptable y riesgo residual.

8.8 Visión general del proceso de aceptación del riesgo

Después de la definición del plan de tratamiento y de que este se juzgue satisfactoriamente, comienza la fase de aceptación del riesgo. Esta fase se refiere de la aceptación formal del plan de tratamiento por la dirección de la organización.

La siguiente figura muestra la fase de aceptación del riesgo.

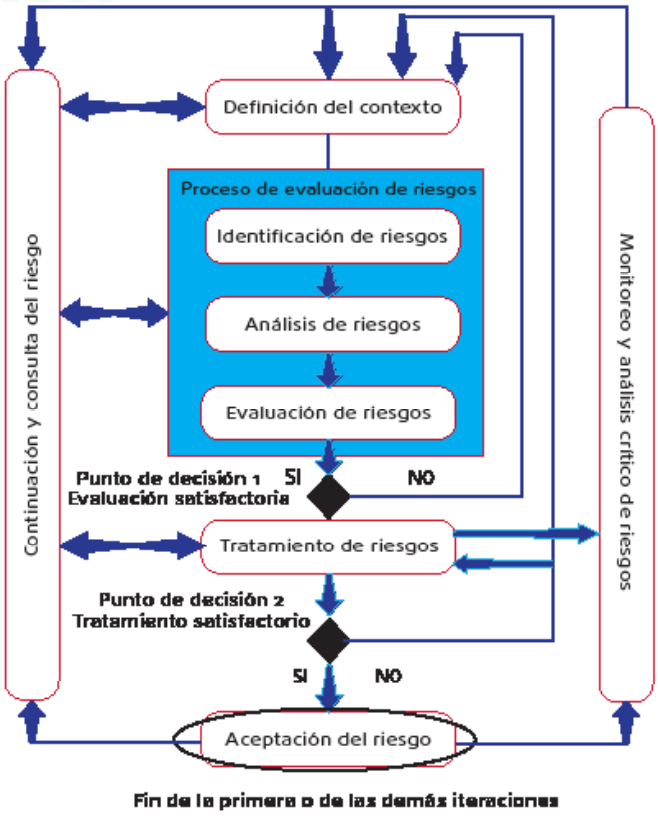


Figura 32. Aceptación del riesgo.

En esta fase de tratamiento del riesgo:

- **Entrada:** plan de tratamiento del riesgo y análisis del riesgo residual.
- **Acción:** decisión formal de aceptación del plan por la dirección de la organización.
- **Salida:** lista de los riesgos asumidos y la justificación de los que no cumplen con los criterios definidos.

8.9 Aceptación del riesgo

En esta fase, la dirección de la organización analizará cuidadosamente el plan de tratamiento del riesgo preparado por el equipo, definiendo en documento formal los riesgos que se aceptarán. La decisión depende de los gestores de la organización, dado que los criterios de decisión son complejos e implican las estrategias de negocio de la organización. Este documento formal hará parte de la llamada "Declaración de aplicabilidad", en el que la organización presenta los controles que no son procedentes y justificados, dado que no se incluirán en el SGSI de acuerdo con la norma ICONTEC NTC ISO/IEC 27001.

Recuerde que el riesgo calculado y tratado adecuadamente es un ingrediente importante del negocio.

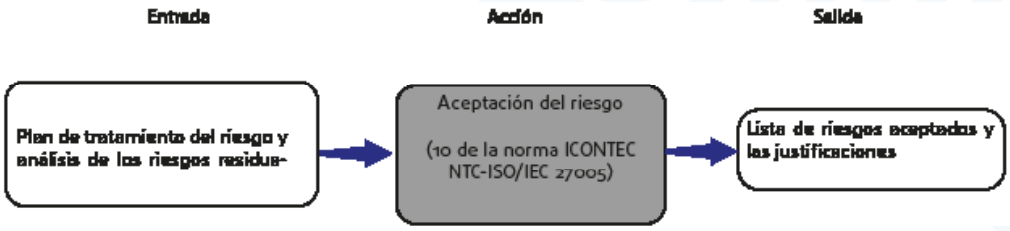


Figura 33. Fase de aceptación del riesgo.

Lectura complementaria

- Sección 9 de la norma ICONTEC NTC ISO/IEC 27005.
- Sección 10 de la norma ICONTEC NTC ISO/IEC 27005.
- Anexo F de la norma ICONTEC NTC ISO/IEC 27005.
- Ítem 5.5 de la norma ICONTEC NTC ISO 31000.

Lo aprendido

- Concepto de tratamiento del riesgo.
- Formas de tratar el riesgo.
- Cómo realizar la aceptación del riesgo.

Capítulo

09

Comunicación y monitoreo del riesgo

Objetivos

Comprender la ejecución del proceso de comunicación y consulta de los riesgos.

Conceptos

Comunicación.

Introducción

Durante todo el trabajo del equipo de análisis del riesgo, hay dos fases que se desarrollan simultáneamente a las demás fases: la comunicación del riesgo y el monitoreo y análisis crítico del riesgo.

Durante todo y cualquier tipo de trabajo, la comunicación es una actividad de gran importancia. Es a través de ella es transmitida la información sobre el desarrollo de las actividades y los resultados obtenidos.

Otra fase de máxima importancia y que se extiende en paralelo a todas las demás fases es el monitoreo y análisis crítico del riesgo. Esta es una fase en que el equipo lleva a cabo el monitoreo y análisis crítico del riesgo y de su trabajo. Una característica de estas dos fases es que son permanentes durante todo el proceso de gestión del riesgo.

Ejercicio de nivelación - comunicación y consulta del riesgo

» ¿Existe algún proceso de comunicación en su organización? Explique.

9.1 Proceso de comunicación y consulta del riesgo de seguridad de la información

La comunicación y la consulta del riesgo es una fase que se desarrolla a lo largo del proceso de análisis del riesgo, desde la primera actividad del equipo de análisis del riesgo. Se trata de un intercambio interactivo, documentado formalmente, continúo e intencional, de información, conocimientos y percepciones sobre cómo se deben gestionar los riesgos.

La comunicación se realiza entre el equipo involucrado y las partes interesadas en las decisiones del proceso de análisis del riesgo, siendo una actividad crítica para el éxito de los trabajos.

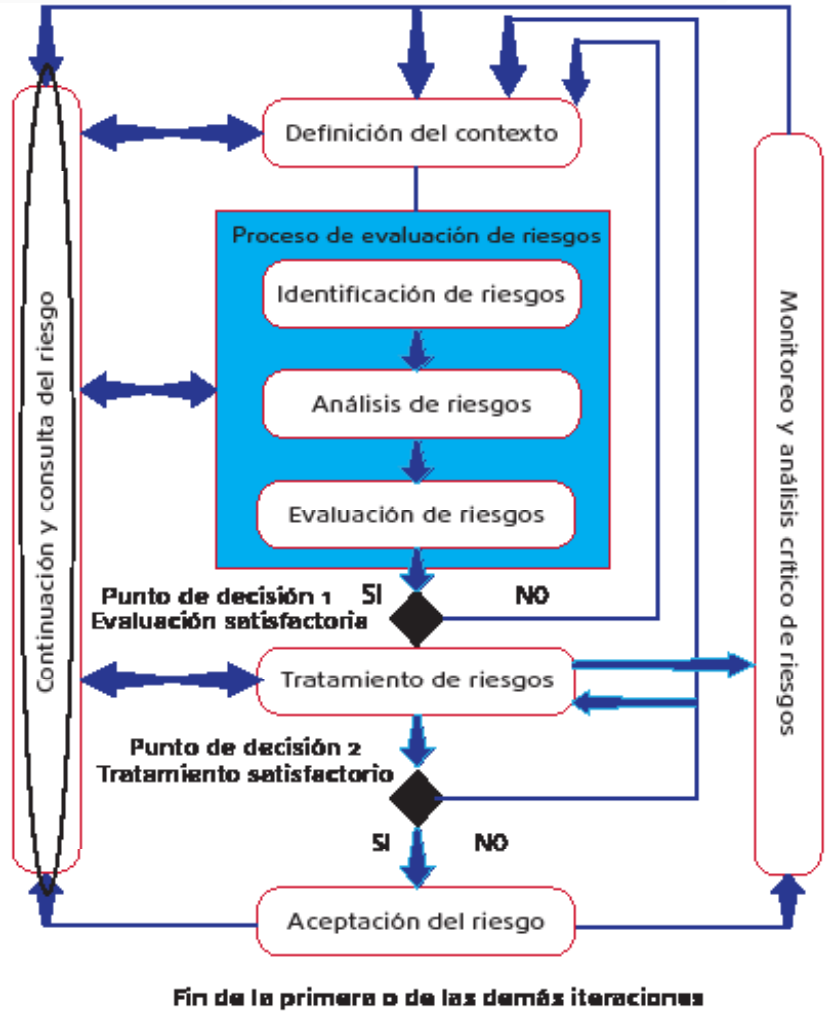


Figura 34. Fase en el contexto del proceso de gestión del riesgo.

En la fase de comunicación y consulta del riesgo el equipo de análisis y la organización tendrán como:

- **Entrada:** Toda la información sobre los riesgos y actividades desarrolladas.
- **Acción:** intercambiar y/o compartir esta información entre el equipo, el tomador de decisión y las partes interesadas.

» **Salida:** comprensión continúa del proceso de gestión del riesgo y de los resultados obtenidos.

Es importante que se lleve a cabo la comunicación durante todo el proceso de gestión del riesgo para mantener actualizadas a las partes interesadas, internas y externas, de manera bidireccional, de modo que las decisiones sean tomadas con conocimiento de causa sobre el nivel del riesgo y la necesidad de tratamiento.

9.2 Comunicación y consulta del riesgo de seguridad de la información

Las actividades de esta fase son ejecutadas durante todo el proceso de análisis de riesgos, debiendo contener el máximo posible de detalles sobre los riesgos encontrados, tales como:

» La existencia de la amenaza, vulnerabilidad y riesgo;
» La naturaleza y forma de la acción;
» La estimativa de probabilidad;
» Su severidad y posibles consecuencias;
» Tratamiento y aceptación del riesgo.

La comunicación permitirá una comprensión adecuada y una mayor agilidad en la toma de decisiones para la implementación de mecanismos de control del riesgo, a fin de evitar daños más graves. Por otra parte, permitirá una mejor percepción de los riesgos y de los beneficios de su rápido tratamiento, así como realizar un trabajo de concientización acerca de la gestión del riesgo y la seguridad de la información.

Una forma de lograr esta comunicación es integrar al equipo un profesional de la organización como punto focal, dejándole el seguimiento de los trabajos y acciones iniciales de comunicación. Otra forma es el equipo realizar regularmente (semanal, quincenal, dependiendo del alcance del análisis) una reunión de seguimiento con los gestores de la organización y presentar los resultados hasta ese momento.

Ejercicio de refuerzo - comunicación y consulta de los riesgos

» Durante el proceso de análisis del riesgo, al identificar una vulnerabilidad grave y de alto riesgo, ¿cuál es su actitud con esta información? Justifique.

Comunicar es también dar un retorno (*status*) sobre la gestión del riesgo para el equipo, para la dirección de la organización y todas las partes interesadas. La creación de informes es una forma de comunicación que permite que la información reunida sea difundida y utilizada en la toma de decisiones.

La sección 11 de la norma ICONTEC NTC ISO/IEC 27005 presenta otros detalles de la comunicación del riesgo.

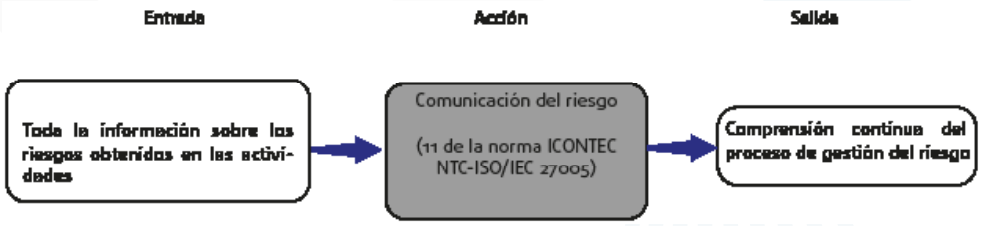


Figura 35. Comunicación del riesgo.

Lectura complementaria

- Sesión 11 de la norma ICONTEC NTC ISO/IEC 27005.
- Sesión 12 de la norma ICONTEC NTC ISO/IEC 27005.

Lo aprendido

- Concepto de la comunicación del riesgo.
- Qué se debe comunicar.
- Cómo hacer la comunicación del riesgo.

Capítulo

10

Monitoreo del riesgo

Objetivos

Ejecutar el monitoreo y análisis del riesgo.

Conceptos

Monitoreo del riesgo y análisis crítico.

Introducción

Paralelamente a las etapas del análisis del riesgo ocurre también una etapa importante para la verificación y control de los resultados del trabajo: la etapa del monitoreo.

La ejecución de esta etapa durante toda la realización del proyecto permitirá que la organización y equipo acompañe la eficiencia de los resultados y la eficacia de los controles.

Ejercicio de nivelación - monitoreo del riesgo

» ¿Cómo se realiza el monitoreo en su organización? Explique.

10.1 Proceso de monitoreo y análisis crítico del riesgo de seguridad de la información

El monitoreo puede ser definido como la continua observación y registro regular de las actividades y acciones de la gestión del riesgo. Es un proceso sistemático de recopilación de información de la gestión del riesgo en todos sus aspectos. Monitorear es verificar y acompañar el progreso de las actividades de la gestión del riesgo, es decir, una observación sistemática, regular y con propósito de verificar el desarrollo de la gestión del riesgo.

El análisis crítico es una evaluación general y detallada sobre los resultados y acciones de la gestión del riesgo en relación con los requisitos pre-establecidos, con el objetivo de hacer el levantamiento y la identificación de problemas y áreas de mejoría para resolver los problemas y mejorar continuamente el proceso de gestión del riesgo.

Esta fase se convierte simultáneamente en la otra fase de la gestión del riesgo. Durante todo el proceso de gestión del riesgo, el equipo de análisis estará también realizando actividades de monitoreo y análisis crítico con el fin de hacer las correcciones necesarias a la brevedad posible.

Durante esta fase son ejecutadas dos actividades:

- Monitoreo y análisis crítico de los factores de riesgo;
- Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo.

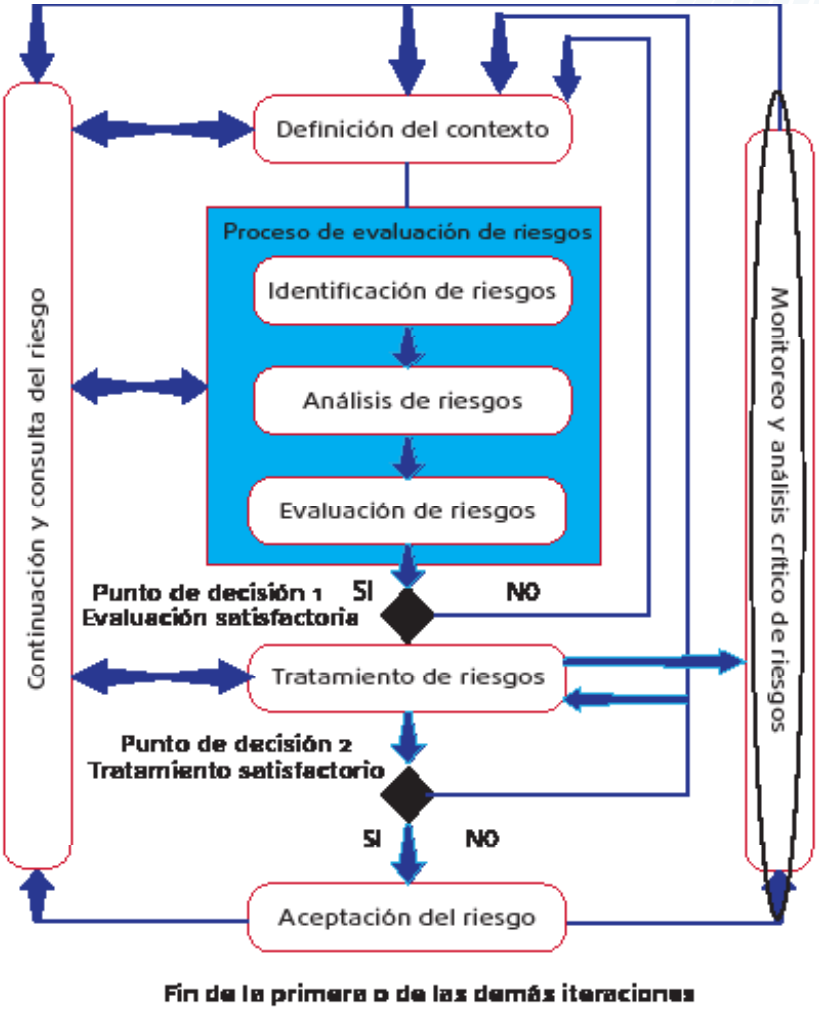


Figura 36. Fase de monitoreo y análisis crítico del riesgo en el proceso de la gestión del riesgo.

10.2 Monitoreo y análisis crítico de los factores del riesgo

El monitoreo es la actividad de identificar y asegurar el control del riesgo, monitoreando riesgos residuales e identificando nuevas amenazas, vulnerabilidades y riesgos, asegurando la ejecución de los planes de tratamiento del riesgo y evaluando su eficiencia y eficacia en la reducción de los riesgos. El equipo debe estar atento a la dinámica de los riesgos y amenazas. Los buenos procedimientos de monitoreo y el análisis crítico de los riesgos proporcionan información que apoyan una toma de decisiones eficaz en relación la aparición de nuevas ocurrencias de los riesgos.

De la actividad de monitoreo y análisis crítico, el equipo de análisis tendrá como:

- **Entrada:** toda la información sobre los riesgos obtenidos y las actividades desarrolladas;
- **Acción:** es la realización de los procedimientos de monitoreo y análisis crítico para la identificación de eventuales cambios en el contexto y el mantenimiento de una visión general de los riesgos.
- **Salida:** la alineación continúa de la gestión del riesgo con los objetivos de negocios y con los criterios de aceptación del riesgo.

El seguimiento del dinamismo de los riesgos y amenazas se debe hacer a través del monitoreo de los activos, vulnerabilidades, probabilidades, entre otros, para que sea posible la rápida identificación de cualquier cambio. En este tipo de actividad, la contratación de los servicios de terceros para monitorear puede representar para la organización una ganancia de eficiencia en la respuesta a las nuevas amenazas que puedan surgir.

Los resultados del monitoreo serán utilizados como datos de entrada para la realización de un análisis crítico, que debe ser hecho por la alta dirección de la organización en el nivel estratégico, para verificar que la gestión del riesgo está cumpliendo con los objetivos de negocio de la organización. En el proceso de análisis del riesgo, el equipo de análisis debe identificar los problemas y los puntos de atención que necesitan mejorar.

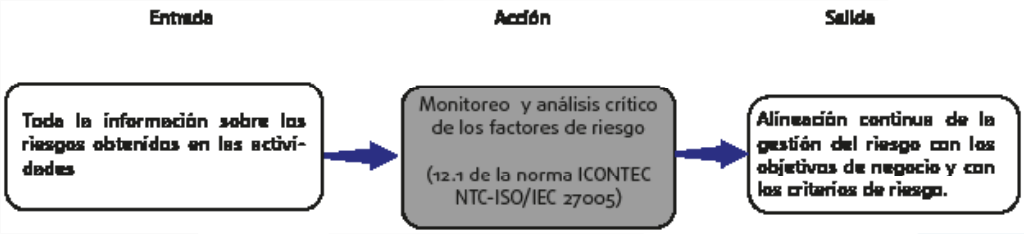


Figura 37. Actividad de monitoreo y análisis crítico.

Ejercicio de refuerzo - monitoreo y análisis crítico del riesgo

» ¿Qué es el monitoreo y análisis crítico del riesgo? Explique su propósito.

10.3 Monitoreo, análisis crítico y mejoramiento del proceso de la gestión del riesgo

Esta actividad tiene por objetivo garantizar que el proceso de gestión del riesgo esté realmente satisfaciendo a los requisitos estratégicos del negocio de la organización.

En la actividad de monitoreo, análisis crítico y mejora del proceso de gestión del riesgo:

» **Entrada:** información sobre los riesgos obtenidos y actividades desarrolladas.
» **Acción:** monitoreo, análisis crítico y mejora del proceso de gestión del riesgo de seguridad de la información.
» **Salida:** la garantía permanente de la relevancia del proceso de gestión del riesgo de seguridad para los objetivos de negocio de la organización o la actualización del proceso.

Esta actividad permite que la organización analice su proceso de gestión del riesgo y la posibilidad de ejecución de las mejoras necesarias para el proceso. En esta actividad, el trabajo del equipo de análisis debe haber realizado la actividad anterior y haber pasado los resultados a la organización, para que sean utilizados como subsidios para el monitoreo, análisis crítico y mejora del proceso de gestión del riesgo para toda la organización.

El monitoreo permite que la organización verifique que todos los recursos necesarios para la gestión y tratamiento del riesgo están disponibles, así como la verificación de la necesidad de cambios en los criterios, en la metodología o en las herramientas utilizadas.

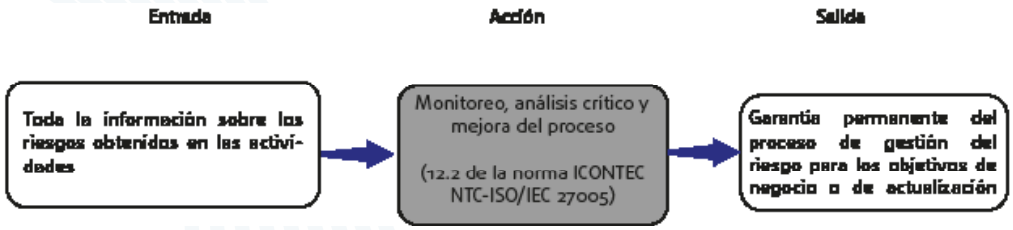


Figura 38. Actividad monitoreo, análisis crítico y mejora del proceso de gestión del riesgo.

Lectura complementaria

» Sesión 12.1 de la norma ICONTEC NTC ISO/IEC 27005.
» Sesión 12.2 de la norma ICONTEC NTC ISO/IEC 27005.

Lo aprendido

» Concepto de monitoreo, análisis crítica y mejora de procesos.
» Razones para llevar a cabo el monitoreo.
» Actividades para llevar a cabo el monitoreo.
» Razones para ejecutar el análisis crítico y la mejora continua.

Cuaderno de actividades

Capítulo

11

11.1 Guía de actividades 1

Actividad 1 – Conociendo conceptos

Para cada concepto a continuación, explique y presente un ejemplo basado en la organización en que usted trabaja. Justifique su respuesta:

Tabla 9. Ejercicio conociendo conceptos

Concepto	Definición	Ejemplo	Justificación
Riesgos de seguridad de información			
Identificación de riesgos			
Impacto			
Reparto del riesgo			
Evitar el riesgo			
Comunicación del riesgo			
Estimación del riesgo			
Tratamiento del riesgo			
Aceptación del riesgo			

Actividad 2 - Conociendo la norma

1. Describa cómo está organizada la norma ICONTEC NTC-ISO/IEC 27005, citando sus secciones.

2. Explique cómo están estructuradas las actividades de las secciones 7-12 de la norma ICONTEC NTC-ISO/IEC 27005.

Actividad 3 - Identificando el proceso

1. Describa la secuencia de las etapas en el proceso de gestión del riesgo.

Actividad 4 - factores críticos

1. ¿Qué es la gestión del riesgo de seguridad de la información y cómo se aplica en su organización?

2. ¿Cuáles son los factores críticos de éxito? Dar ejemplos basados en su organización.

3. En su opinión, ¿cuál es la importancia de la comprensión de la gestión del riesgo para llevar a cabo nuestras actividades diarias?

11.2 Guía de actividades 2

Visión general de la actividad

Serán realizadas las actividades necesarias para la "definición del contexto". La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de gestión del riesgo.

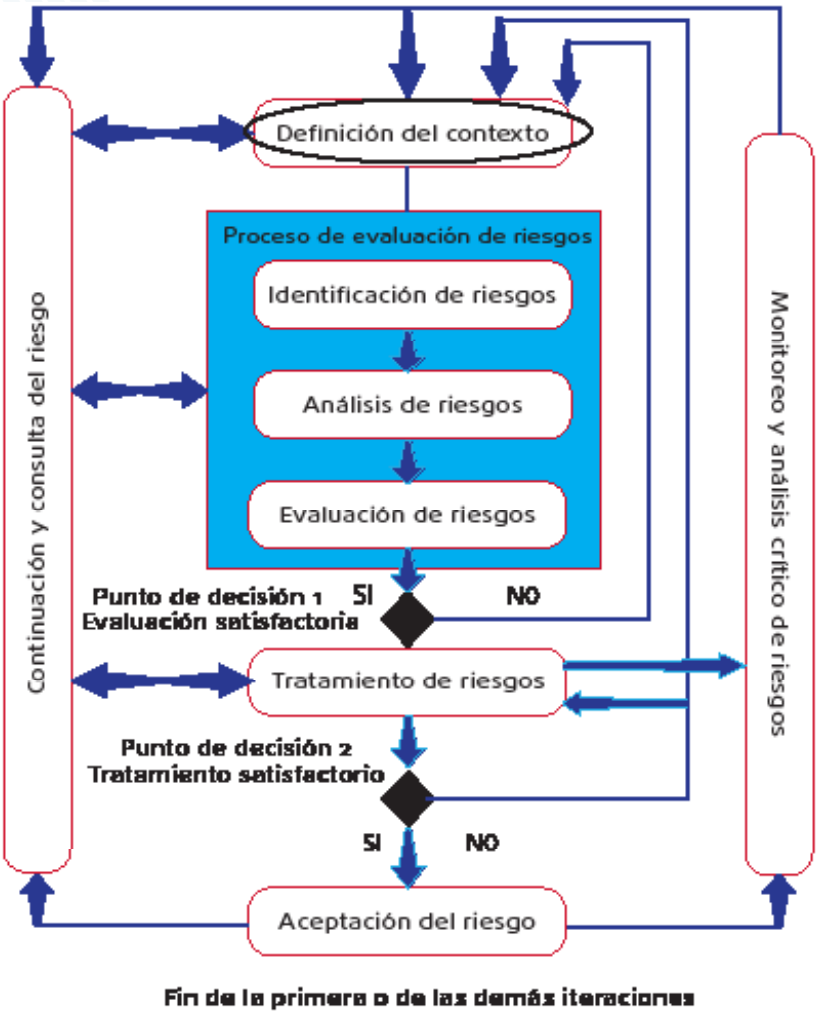


Figura 39. Actividades para la "definición del contexto".

La realización de esta actividad debe ser acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, el apoyo prestado y también por la experiencia y conocimientos en su organización.

Para esta actividad, los estudiantes deben hacer uso del apéndice A (descripción de la organización), que permitirá la creación de una organización ficticia o ayudar en algunas observaciones acerca de su organización. La hoja de trabajo de esta actividad consiste en preguntas básicas para entender el contexto organizacional.

La secuencia de las actividades será:

1. Lectura de la sección 7 y el Apéndice A de la norma ICONTEC NTC-ISO/IEC 27005;

2. Lectura del caso A (descripción de la organización) de este cuaderno de actividades;

3. Explicación y demostración por parte del instructor de la Tabla 10 de análisis del riesgo.

Tabla 10. Analizar la organización y el contexto

Objetivo principal de la organización	
Organización empresarial	
Misión	
Valores	
Estructura de la organización	
Organigrama	
Estrategias	
¿Cuál es el sector que ha solicitado el proyecto? ¿Cuál es su nivel jerárquico dentro de la organización?	
¿Cuáles son los principales procesos de negocio en la organización?	
¿Cuáles son los requisitos legales o reglamentarios?	
¿Cuáles son sus principales productos?	
¿Cuáles son sus principales proveedores?	
¿Cuál es el número total de empleados? ¿Cómo se subcontratan?	
¿Cuáles son los requisitos de las políticas internas de la organización?	

Sólo pase a la guía siguiente cuando haya terminado.

4. Ejecución de las actividades de la definición del contexto:

a. Ejercicios de la guía "definir contexto"

El objetivo de esta actividad es, a través de repuestas a algunas preguntas, desarrollar en el estudiante la comprensión de lo que debe ser pensado, planificado y comprobado para definir el contexto.

Debe responder a las preguntas que permitirán que el equipo de análisis del riesgo identifique y entienda el contexto del ambiente donde será desarrollará el análisis.

Para cada tópico deberán ser colocadas a la derecha las observaciones o justificación correspondientes.

Sólo pase a la guía siguiente cuando haya terminado.

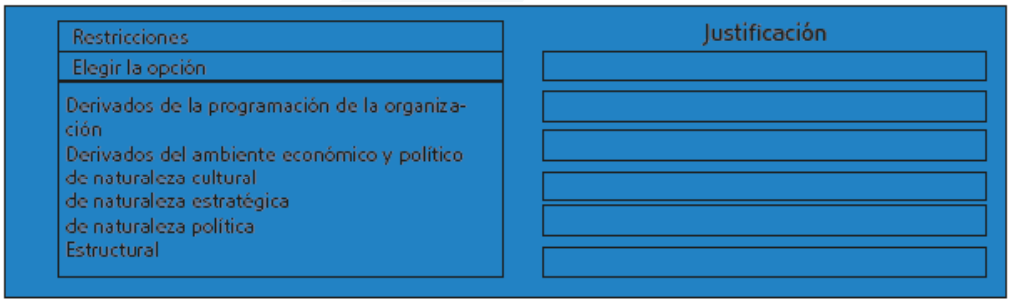
b. Ejercicios de la guía: "restricciones"

Esta actividad conduce a la comprensión de la importancia de la identificación de restricciones existentes.

En esta guía se introducirán las restricciones aplicables a la organización, de acuerdo con el apéndice A de la norma ICONTEC NTC- ISO/IEC 27005.

La columna "restricciones" presenta una lista basada en la norma, dejando al estudiante a elegir las que se aplican y escribir la justificación.

Figura 40.
Análisis de las restricciones.



Hay restricciones que afectan a la organización y restricciones que afectan el alcance de la gestión del riesgo.

Tabla 11. Análisis de restricciones

	Tipo de restricciones	Justificación
Restricciones que afectan a la organización	Que surgen de la agenda de la organización	
	Que surgen de la situación económica y política de la agenda de la organización	
	De carácter cultural	
	De carácter estratégico	
	De carácter estratégico	
	De carácter político	
	Estructural	
	Funcional	
	Presupuesto	
	Métodos relacionados	
	Relativas a los recursos humanos	
	Territorial	

	Tipo de restricciones	Justificación
Restricciones que afectan el alcance	Ambiental	
	Financiera	
	Organizacional	
	Temporal	
	Derivadas de los procesos existentes	
	Métodos relacionados	
	técnicas	

a. Ejercicios de la guía: "alcance"

El objetivo de esta actividad es, a través de repuestas a algunas preguntas, desarrollar en el estudiante la comprensión de lo que debe ser pensado, planificado y comprobado para definir el alcance y sus límites.

Esta guía presenta ejercicios para que el equipo de análisis tenga una perfecta comprensión de los alcances y sus límites. Para cada tópico deberán ser colocados a la derecha las observaciones correspondientes.

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicios de la guía: "criterios"

Esta guía presenta un ejercicio para permitir la definición de los criterios que serán trabajados durante todo el análisis del riesgo.

Aquí el equipo de análisis del riesgo de la organización que realizará el trabajo, definirá los criterios para el desarrollo de los trabajos durante todo el proceso. Es importante que estos criterios sean viables y válidos para el ambiente del alcance de la gestión del riesgo y para la organización.

Criterios a ser definidos:

- **Probabilidad:** representa el porcentaje de posibilidades de que ocurra un evento.
- **Relevancia del activo:** importancia del activo para los negocios/servicios de la organización.
- **Gravedad de las consecuencias:** grado de las consecuencias sufridas por un activo en relación a los servicios/negocio (proporcionado por el activo o pasar a través de ella) al ser atacado o dejar de funcionar;
- **Impacto:** índice para medir la cantidad de daños o costos a la organización causados por la ocurrencia de un evento de seguridad de la información;
- **Criterio del riesgo:** define el nivel o su escala de aceptación de los riesgos y depende de las políticas, objetivos y metas de la organización.

Tabla 12. Definición de criterios.

Impacto	
Nivel	**Descripción**
Despreciable	De acuerdo con la organización – Defina
Bajo	De acuerdo con la organización – Defina
Significativo	De acuerdo con la organización – Defina
Importante	Afectan la imagen de la organización y causan interrupción de 12 horas en los negocios. La organización deja de funcionar/producir por 12 horas.
Desastre	De acuerdo con la organización – Defina

Cada criterio es compuesto por nivel y descripción. Para cada uno de ellos el equipo de análisis deberá definir sus criterios.

Para la actividad, las descripciones que posee la palabra DEFINA deberán ser contempladas por el equipo, y algunos niveles podrán ser alterados. Los criterios definirán las demás actividades durante el curso.

5. Comprobación y corrección por parte del instructor.

   Al concluir la "Guía de Actividades 2", el equipo de análisis conocerá el ambiente de la organización. El alcance del análisis estará definido, así como los criterios de análisis que guiarán todos los trabajos de la gestión del riesgo.

Caso A - Descripción de la organización

La organización

Con sede en la ciudad de Bogotá, una oficina comercial ubicada en Medellín y otra oficina en Barranquilla, la KWX Industria Gráfica y Servicios LTDA opera en el mercado desde 1998. Actualmente cuenta con aproximadamente 230 empleados. Posee equipos de alta tecnología y el objetivo de producir y distribuir productos y servicios con patrón de calidad internacional, atendiendo al mercado de organizaciones del sector educativo.

La organización tiene una pequeña participación en el mercado nacional, con una facturación media de US$ 45.000.000 anuales. Tiene como meta duplicar su participación en el mercado en tres años, KWX planea la reestructuración de sus procesos internos y también la reformulación de su cultura, visando la seguridad de la información y la preparación para la certificación ISO 27001. Actualmente posee la certificación ISO 9001 obtenida hace dos años.

Visión

La alta administración tiene la intención de mejorar su forma de trabajar, reduciendo costos y buscando conservar e invertir en su activo intelectual y parque tecnológico, trabajando en la busca de la mejora continua y de la excelencia operacional, para establecerse cada vez más como una marca de éxito.

La visión de KWX es ser una marca de expresión nacional, ganando el público a través de productos innovadores, relaciones éticas con socios y la comunidad, y la práctica constante de la responsabilidad social, dando prioridad a la preservación ecológica.

A pesar de todo esto, la KWX también apuesta por el factor humano y tiene en cuenta la satisfacción de sus funcionarios y colaboradores. "La satisfacción personal es algo que tratamos de ofrecer a nuestros funcionarios. Nosotros queremos que sean algo más que solos empleados, pero que vengan para KWX contentos y orgullosos de ser parte de esta compañía ", dice el director presidente.

Estructura organizacional

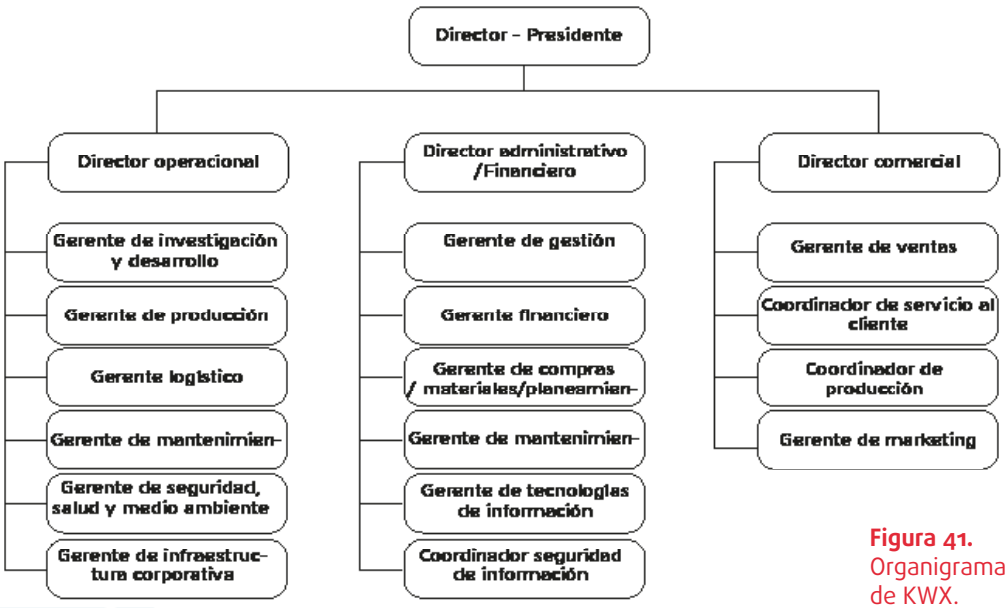


Figura 41. Organigrama de KWX.

Dirección Operacional

Investigación y desarrollo

La KWX está siempre en busca de nuevas tendencias y tecnologías para ser una referencia en el mercado nacional de cursos reconocidos. La elaboración de nuevos cursos y productos, en línea con las tendencias del mercado y la competencia, son de vital importancia para el éxito de la organización. Es en este departamento que las nuevas ideas, materiales y productos son diseñados, además de mejoras en el proceso de fabricación de los productos existentes. Todos los análisis de los nuevos cursos y folletos se realizan en este departamento, que es el principal capital intelectual de la organización, por lo tanto debe ser protegido de todas las maneras.

Producción

La planificación de la producción se realiza con base en la información recibida por el área de servicio al cliente, y también de acuerdo al historial de producción de los últimos dos años. Para el buen funcionamiento de la planificación, es necesaria una gran interacción con las áreas de servicio al cliente, compras, ventas, control de materiales (almacén) y, especialmente, con las áreas de la fábrica. El área de planificación genera un programa de producción para los próximos 5 días, aunque este programa se revisa y se actualiza diariamente.

Almacén

Responsable de la recepción de los materiales, más el *stock* de productos que se consideran esenciales para el funcionamiento del proceso de fabricación. Materiales de oficina también se encuentran en el almacén.

Logística

Área responsable de todo el movimiento de productos dentro y fuera de la organización, definiendo la estrategia de distribución de los productos para los clientes. Asegura que el producto sea entregado a su destino final, a tiempo y especificaciones correctas. Aún controla el movimiento de los productos y materiales en la fábrica.

Mantenimiento

Incluye el mantenimiento eléctrico y mecánico. El equipo de mantenimiento trabaja durante horario administrativo, asignado a un empleado en cada turno para acompañar y resolver eventuales problemas en el proceso de producción. El mantenimiento tiene la responsabilidad de mantener todas las máquinas en funcionamiento, además de los eléctricos, aire acondicionado, alarmas y trinquetes de la fábrica, cuidando aún del mantenimiento preventivo.

Seguridad, salud y medio ambiente

El área de la seguridad ambiental abarca los siguientes elementos: salud ocupacional, seguridad patrimonial y medio ambiente, además de la integridad de los funcionarios. Es responsable por las normas ambientales, la relación con las agencias ambientales, la aplicación de las herramientas y procedimientos de seguridad, la realización de mapas de riesgo de las áreas de la organización, e incluso la definición y adopción de los EPI´s (Índices de Desempeño Ambiental) usados por los empleados.

Esta área también es responsable por la definición de la formación y de la concientización de los empleados sobre la importancia de trabajar con seguridad. Esta área es también responsable de la investigación de accidentes e incidentes en la compañía, y de la toma de acciones correctivas para evitar que estos se repitan. Esta es un área de vital importancia para KWX, dado que el cumplimiento de las leyes y la protección del medio ambiente son prioridades para la organización. Importantes inversiones se han hecho en esta área, ayudando a hacer KWX una referencia en los aspectos socios ambientales.

Dirección administrativa-financiera

Gestión humana

Tiene la responsabilidad de la contratación y desvinculación de personal, organización de la formación interna y externa, la gestión de nóminas, control de horarios, almuerzos y beneficios. También es responsable de buscar un promedio de salarios del mercado, programas de promoción de empleados y controlar el programa de incentivos por ganancias de la organización.

Finanzas

Departamento que incluye la parte financiera: tesorería, área fiscal, costos, cuentas por pagar y por cobrar, control y activos fijos. Debido a que es una zona de gran sensibilidad e importancia, el área financiera se apoya en una serie de sistemas y aplicaciones que aseguren el buen funcionamiento de la organización y la fiabilidad de los números y planes de cuentas presentadas.

Compras y materiales

Este sector es responsable de todo el proceso de adquisición, desde la negociación con los proveedores hasta la compra final de los productos. Informan sobre los precios medios de mercado a determinados empleados para que puedan hacer una solicitud de pedido. Los empleados que no son del área de compras no pueden tener contacto con los proveedores. Los contratos también se negocian por el área de compras.

Dirección comercial

Ventas

Área responsable de la planeación del volumen de ventas que deben realizarse en el mes, a partir de datos recibidos del personal de planeación de la producción, y también responsable de estimar los pedidos de los clientes. El área de ventas es responsable de todo el proceso de venta de productos de la compañía, así como la relación con los clientes, que son las instituciones educativas que comercializan la línea KWX. Esta área también ofrece soporte técnico a los usuarios finales, así como información para el mantenimiento de la página web de la compañía.

Mercadeo

Área responsable del desarrollo de la estrategia para la comercialización y distribución de la línea de productos KWX. Coordina campañas publicitarias en diferentes medios de comunicación, además de desarrollar y actualizar el sitio web de la organización.

Infraestructura

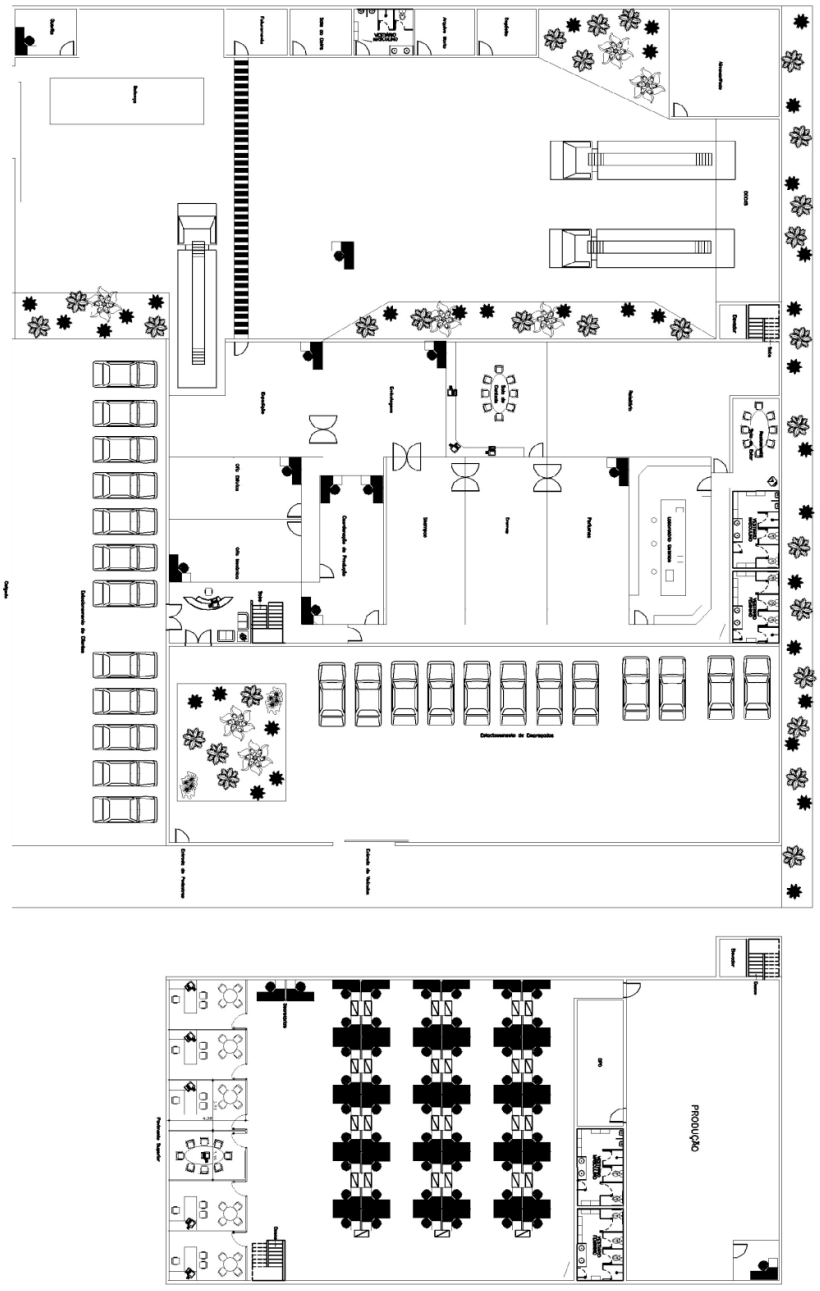


Figura 42. KWX planta actual - Fábrica.

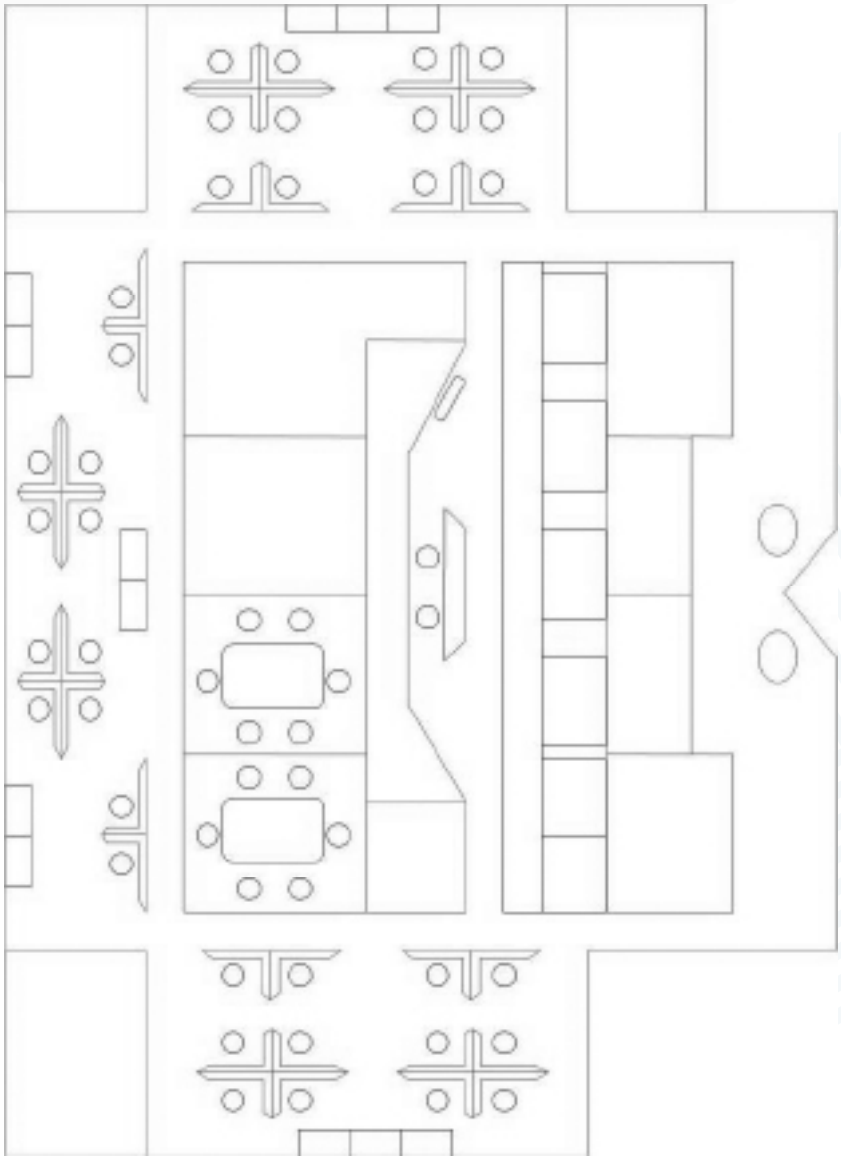


Figura 43. Planta KWX - oficina comercial.

11.3 Guía de actividades 3

Visión general de la actividad

Después de identificar el ambiente, definir el alcance y definir los criterios, el equipo de análisis del riesgo es ahora capaz de iniciar la etapa de identificación de los riesgos, ejecutando las actividades necesarias para la "Identificación de los riesgos: amenazas, activos y controles existentes."

La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de gestión del riesgo:

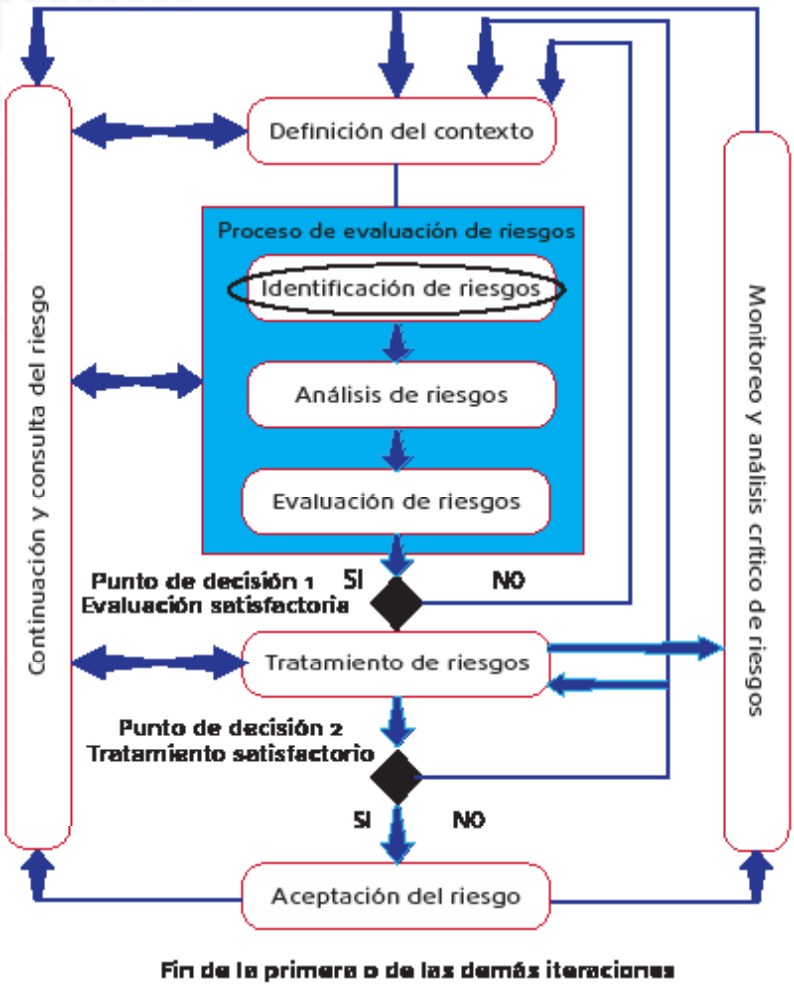


Figura 44. Actividades del proceso de gestión del riesgo. Identificación del riesgo

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo previsto y por la experiencia en su organización.

Para esta actividad el estudiante debe hacer uso del "Caso B" (Infraestructura), que permitirá el levantamiento de los equipos, procesos, personas y tecnologías de la organización KWX.

Secuencia de actividades:

1. La lectura de las secciones 8.1, 8.2 y hasta B.1 del Anexo A de la norma ICONTEC NTC-ISO/IEC 27005;
2. Lectura del "Caso B" (Infraestructura) de este cuaderno de actividades;
3. Explicación y demostración de la Tabla 13 de análisis del riesgo por el instructor;
4. Ejecución de las actividades de las tablas:

En esta guía se encuentran tres tablas:

1. La tabla "Activos"
2. La tabla "Amenazas"
3. La tabla "Controles Existentes"

a. Ejercicio de la guía "Activos" - Identificar los activos del alcance del análisis del riesgo. En este ejercicio el equipo de análisis enumerará todos los activos de la organización que están dentro del alcance del análisis del riesgo, que se dividen en dos grupos: activos primarios y activos de soporte e infraestructura. Cada activo enumerado deberá justificarse.

Deberán ser enumerados 20 activos, siendo 10 primarios y 10 de soporte e infraestructura.

Tabla 13. Identificación de activos del alcance del riesgo

		Justificación/Evidencias
Activos primarios	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
		Justificación/Evidencias
Activos de soporte e infraestructura	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	

Sólo pase a la guía siguiente cuando haya terminado.

b. El ejercicio de la guía "Amenazas" - Identificación de las amenazas a los activos.

Con los activos ya identificados y conocidos, el equipo de análisis ahora identificará todas las amenazas relacionadas con los activos planteados.

Para realizar el ejercicio, se deben enumerar apenas dos amenazas para cada activo, pero recuerde que en una actividad práctica real todas las amenazas deberán enumerarse. Como una ayuda para ello, se utilizará el Apéndice C (Ejemplos de amenazas comunes) de la norma ICONTEC NTC-ISO/IEC 27005.

En nuestro ejercicio, los activos listados en la actividad anterior serán utilizados para la guía "amenazas", que aparece junto a una lista de amenazas para que sean seleccionadas las amenazas que pueden venir afectar a cada activo. Asegúrese de justificar sus elecciones.

Sólo pase a la guía siguiente cuando haya terminado.

Tabla 14. Identificación de las amenazas a los activos

Activos	Amenaza 1	Amenaza 2	Justificación/ Evidencias
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

Continuación tabla 14. Identificación de las amenazas a los activos

Activos	Amenaza 1	Amenaza 2	Justificación/ Evidencias
15			
16			
17			
18			
19			
20			

Tipos de amenazas	
Fuego	La divulgación indebida
Contaminación	Los datos de fuentes no confiables
Accidente grave	Cambio del hardware
La destrucción de los equipos o medios	Cambio Software
El polvo, la corrosión, congelación	La determinación de la ubicación
Fenómeno climático	Falla del equipo
Fenómeno sísmico	El equipo defectuoso
Fenómeno volcánico	La saturación del sistema de información
El fenómeno climático	Defecto Software
Inundaciones	La violación de las condiciones de utilización del sistema de información que permite el mantenimiento
La falta de aire acondicionado o sistema de suministro de agua	El uso no autorizado de equipos
La interrupción de la fuente de energía	La copia ilegal de software
El fallo de los equipos de telecomunicaciones	Utilice copias de software falsificado o ilegal
La radiación electromagnética	Compromiso de Datos
La radiación térmica	Procesamiento de datos ilegal
Pulsos electromagnéticos	Error durante el uso
La interceptación de señales interferentes comprometer	Abuso de derecho
Distancia de Espionaje	Derechos de forja
El robo de los medios de comunicación o documentos	Repudio de Acciones
El robo de equipos	Falta de disponibilidad de los recursos humanos
Recuperación de los medios de comunicación reciclar o desechar	

c. Ejercicio de la guía "Controles existentes" - Identificación de los controles existentes o con implementación planeada.

Con los activos y amenazas ya identificados por el equipo de análisis, la siguiente actividad es identificar los controles existentes y los que están en proceso de implementación. Para cada amenaza identificada y para cada activo, el equipo de análisis del riesgo debe identificar si ya hay controles implementados o que están previstos para ser implementado. Esto se hace con el fin de asegurar que estos controles sean recomendados nuevamente en el futuro.

En este ejercicio deberán ser presentados dos controles para cada amenaza identificada, (en caso que existan). Para cada activo deben ser identificados por lo menos cuatro controles. En realidad este número puede ser variable para cada activo. Estos controles no deben necesariamente estar relacionados con las amenazas listadas en la etapa anterior. Si no existir control implementado o a ser implementado, sólo hay que poner la respuesta "No existe".

Las respuestas de las guías anteriores son copiadas en esta guía. Para cada tópico deberán ser colocadas a la derecha las justificaciones correspondientes.

Tabla 15. Identificación de controles existentes

Activos	Amenaza	Control existente	Justificación/ Evidencias

5. Verificación y corrección por parte del instructor.

   Al completar la "Guía de actividades 3", el equipo de análisis tendrá una lista que contiene los activos, las amenazas que afectan o pueden afectar a cada activo y los controles actualmente existentes o previstos para ser implementados.

Caso B - Infraestructura

Infraestructura física

La seguridad física es mantenida por un equipo de profesionales relacionados a la seguridad patrimonial.

La seguridad física/patrimonial de la KWX incluye los siguientes activos:

- Portería/Caseta de vigilancia: dos puertas para el control de acceso (sin operación), 5 guardias contratados de la organización GuarFull24;
- Parqueaderos: puertas electrónicas puertas (dos sin operación) y cercas eléctricas;
- Centro de datos: control de acceso a través de llaves, aspersores y racks desbloqueados;
- No hay sala de seguridad;
- Puestos de trabajo sin controles específicos.

Infraestructura tecnológica

El departamento de las TI está subordinado al director administrativo-financiero. También es responsable por la creación del área de la seguridad de la información. Asigna dos profesionales en funciones multitarea, que se turnan en las tareas del día a día, como por ejemplo *help desk*, administración de la red, creación y eliminación de cuentas de usuario, entre otros.

Activos de tecnología

La estructura soportada por el departamento de las TI de KWX actualmente comprende:

- 750 usuarios con acceso a la red y correo electrónico;
- 800 máquinas (siendo 550 *notebooks*);
- 25 impresoras;
- Redes Windows;
- Redes de Linux;
- 1 servidor de correo electrónico Windows Exchange;
- 6 servidores de archivos;
- 6 servidores de *backup*;
- 1 servidor web para soporte del ambiente del comercio electrónico vía Internet;

- 1 servidor DNS;
- 5 *firewalls*;
- 3 roteadores para acceso a internet (una en cada sed);
- 4 *switches core* para soporte a la infraestructura de acceso a la internet;
- 1 PABX que contiene extensiones analógicas y digitales (total de 1.200 sucursales, siendo 300 con identificador de llamadas para la fábrica);
- 1 PABX que contiene las extensiones digitales (total de 400 sucursales, todas con identificador de llamadas a la oficina);
- 7 salas de reuniones con conexión de red inalámbrica, videoconferencia y proyector;
- 1 servidor dedicado para el sistema ERP;
- Servidor de correo/antivirus (Linux Debian);
- Servidor de Proxy (Linux Debian);
- Servidor ADM/Intranet (Windows 2000 Server/IIS);
- Servidor Unix Criación (AIX 4);
- 10 puestos de trabajo (Windows 2003);
- 35 puestos de trabajo (Windows 8 profesionales);
- 20 puestos de trabajo (Windows 7 Professional);
- 15 puestos de trabajo (Macintosh);
- 100 puestos de trabajo con Ubuntu 12;
- 10 computadoras portátiles (para la dirección, totalmente liberados);
- 6 *switch* (3 con 12 puertas);
- 4 *hubs* (3 con 24 puertas);
- 3 ruteador (Cisco);
- 1 punto de acceso inalámbrico (D-Link);
- Link con internet (1 GB) en cada sed;
- 3 links ADSL de 10 MB inoperantes por falta de uso.

Sistemas de soporte a los negocios

Los siguientes sistemas son soportados por las TI:

- ERP: controla procesos financieros-contables, de fabricación, gerenciamiento de materiales y logística;
- Sistemas de recursos humanos (nómina, control de horario): subcontratado con un proveedor externo;
- Seguridad Patrimonial: sistema de lector de carnet para acceder a las áreas controladas/restringidas;
- Sitio *e-commerce* de KWX: sitio web institucional y de comercio electrónico B2B para las relaciones con clientes y proveedores;
- Intranet: local donde están contenidas las noticias internas de

KWX, su visión y misión, así como todas las políticas, procedimientos y reglas de la organización;
- Sistemas de producción: aplicaciones específicas de cada una de las áreas productivas que trabajan juntas de una manera integrada, así los procesos de producción y planificación de KWX;
- Sistemas de acceso: controles de acceso, bases de datos y registros de las puertas, data center y sala de seguridad;
- Sistema de circuito cerrado de televisión.

Situación actual de la seguridad de la información en la organización

Subordinado al área de las TI, el área de la seguridad de la información cuenta con un profesional que actúa en el papel de coordinador de seguridad de la información, siendo responsable de la preparación y gestión de las políticas y prácticas de seguridad. Trabaja en conjunto con el personal de las TI y también realiza periódicamente auditorías internas, además de trabajos de concientización a los empleados. Este profesional no tiene un alto poder de toma de decisiones y está subordinado al gerente de las TI.

Buscando mayor competitividad, credibilidad y seguridad, KWX contrató a un equipo de consultores de seguridad de información. Esta medida se tomó en base de una investigación realizada por la consultoría de mercado realizada junto con otras organizaciones del mismo segmento, motivados por el objetivo de la internacionalización de la marca en el futuro. Fue definido en la contratación, un trabajo de levantamiento de la situación actual de la organización en términos de seguridad de la información, la comprensión de los procesos, análisis de riesgo, propuestas de mejoría, todo dentro de un alcance definido con la alta gerencia.

11.4 Guía de actividades 4

Visión general de la actividad

Con los activos, las amenazas y los controles ya planteados e identificados por el equipo de análisis, los pasos siguientes son la identificación de las vulnerabilidades y las consecuencias en caso de que estas vulnerabilidades sean explotadas por agentes para la realización de las amenazas. Ahora son realizadas las actividades necesarias para el "Análisis del riesgo – identificación del riesgo: vulnerabilidades y consecuencias." La siguiente figura muestra la ubicación de estas actividades en el proceso de gestión del riesgo:

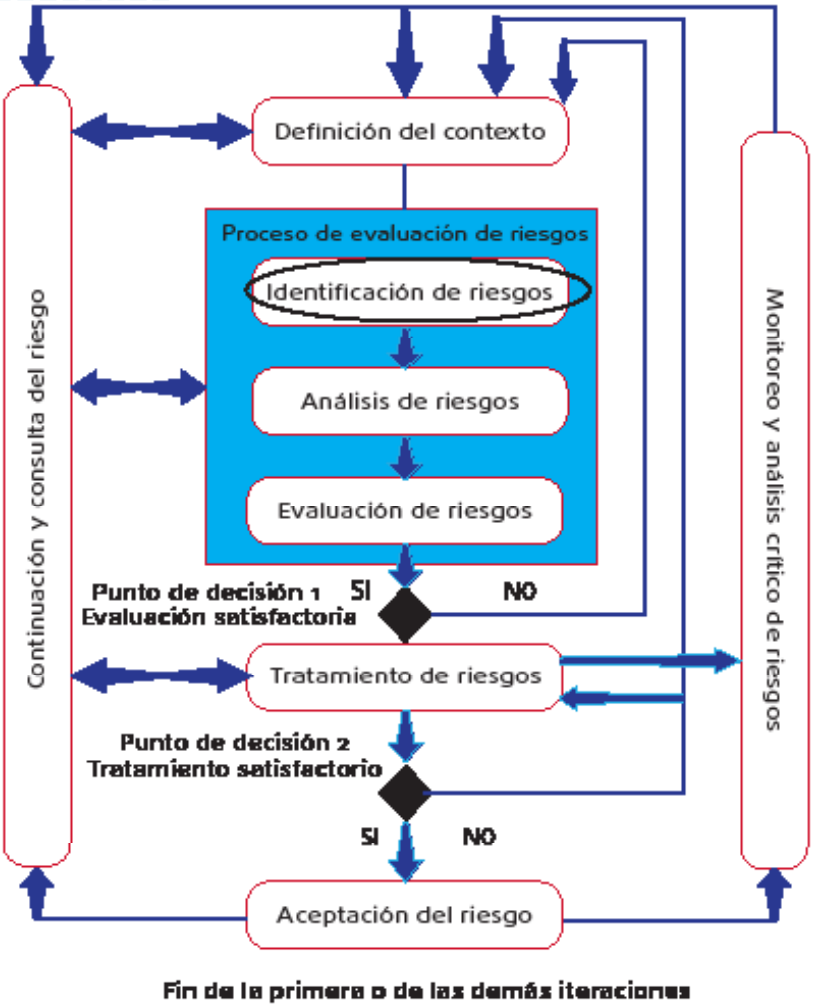


Figura 45. Actividades del proceso de gestión del riesgo. Identificación de vulnerabilidades

La realización de esta actividad debe ir acompañada de la lectura de la norma INCOTEC NTC-ISO/IEC 27005, del material de apoyo suministrado y también por la experiencia en su organización.

Para esta actividad los estudiantes deberán hacer uso del "Caso C" (problemas relatados y observados) que permitirá el levantamiento de los problemas de la organización KWX.

La secuencia de las actividades será:

1. La lectura de las secciones 8.2.1.5, 8.2.1.6 y del anexo D de la norma INCOTEC NTC ISO/IEC 27005;
2. Lectura del "Caso C" (problemas reportados y observados) de estas actividades en el contrato;
3. Explicación y demostración de la Tabla 16 por el instructor;
4. La ejecución de las actividades propuestas;

En esta guía se encuentra las siguientes tablas:

1. Identifique las vulnerabilidades
2. Identifique las consecuencias

a. Ejercicio de la guía "Vulnerabilidades" – Identificación de las vulnerabilidades no atendidas por los controles existentes.

En esta actividad, el equipo de análisis identificará y enumerará las vulnerabilidades existentes para cada activo de la organización.

Con los activos, las amenazas y los controles ya levantados e identificados por el equipo de análisis, la siguiente actividad es identificar las vulnerabilidades y debilidades existentes en estos activos que pueden ser explotadas por los agentes para realizar las amenazas. Para cada vulnerabilidad debe ser presentada la evidencia (justificación).

Para el ejercicio práctico, para cada activo deben ser identificados hasta ocho vulnerabilidades, cuatro para cada amenaza identificada. En realidad este número es variable para cada activo y para cada amenaza.

Tabla 16. Identificación de las vulnerabilidades

Activos	Amenaza	Control existente	Vulnerabilidades encontradas	Justificación/ Evidencias

Para apoyar la actividad, en el "Caso C" de este cuaderno de actividades se presenta fotografías tomadas del ambiente de la organización, dejando al descubierto varias vulnerabilidades.

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicio de la guía "Consecuencias" - Identificación de las consecuencias de las vulnerabilidades levantadas.

En esta actividad, el equipo de análisis va identificar las consecuencias para cada vulnerabilidad, si se produce. Estas consecuencias pueden variar para cada tipo de activo y cada tipo de amenaza. Para cada consecuencia debe ser presentada la evidencia (justificación).

Para el ejercicio, para cada vulnerabilidad identificaremos sólo una consecuencia de una lista predefinida. Esta lista se compone de:

- La pérdida o degradación de la confidencialidad;
- La pérdida o degradación de la integridad;
- La pérdida o degradación de la disponibilidad;
- La pérdida o degradación de la autenticidad;
- La pérdida financiera por reproceso;
- Afecta a la imagen y reputación.

Esta lista es sólo para llevar a cabo el ejercicio. Normalmente, estas consecuencias son específicas para cada tipo de organización. Así como la cantidad de consecuencias para cada vulnerabilidad es también un número variable.

Las respuestas de las guías anteriores son copiadas para esta guía.

Tabla 17. Identificación de las consecuencias

Activos	Amenaza	Control existente	Vulnerabilidades encontradas	Justificación/ Evidencias

Sólo pase a la guía siguiente cuando haya terminado.

5. Verificación y corrección por el instructor.

Al concluir la "Guía de Actividades 4", el equipo de análisis tendrá una lista de los activos, amenazas que afectan o pueden afectar a cada activo, los controles existentes o con vista previa a la ejecución, las vulnerabilidades de cada activo y las consecuencias si estas vulnerabilidades son explotadas por agentes de amenaza.

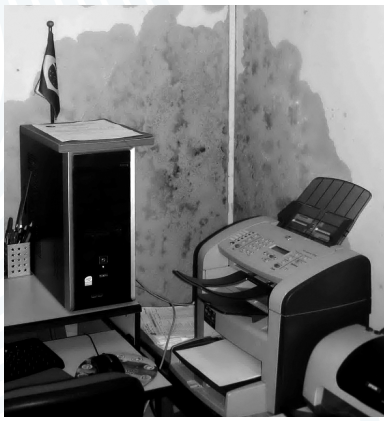
Caso C

A continuación se muestran algunas fotografías tomadas del ambiente de la organización, dejando al descubierto varias vulnerabilidades.

Tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	Situación del ambiente de trabajo en un almacén de Bogotá.
	La conexión entre dos áreas de la misma organización presenta inestabilidad. Los técnicos han utilizados todas las herramientas tecnológicas disponibles, pero no identificaron la causa de la inestabilidad en la línea de producción, que no puede guardar la información en la base de datos.
	Vista lateral de la sede en Medellín.
	Recientemente, el departamento de informática de la organización identificó graves problemas de inestabilidad eléctrica en su red. La sorpresa de los técnicos es que en la sala de servidores no ocurrió ningún problema. El problema sólo ocurrió en el área de almacenamiento de la organización. Los técnicos sospechan de la falta de conocimiento de los operadores del almacén (fuente: http://www.arqcoop.com/patologias-da-construcao/).

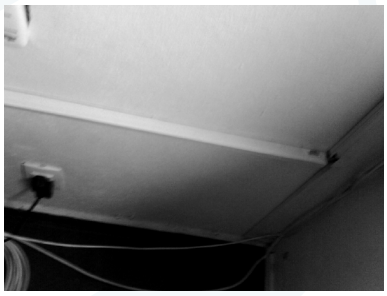
Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	El equipo responsable por el área de las TI de la organización ha sido sorprendida por la falta de acceso a internet. Ellos están buscando lo que puede estar ocurriendo dado que los cables que entran en el edificio por parte del operador están cortados y parte de estos cables fueron robados. (Fuente: http://brazil.indymedia.org/content/2007/02/373244.shtml).
	El departamento de contabilidad tenía problemas de impresión de recibos, y el departamento de recursos humanos no podía emitir la nómina. Tras el análisis de la impresora, se dio cuenta de que no había ningún problema, pero el problema se ha producido en la conexión de red. Los técnicos están trabajando en el local para identificar el motivo. Últimamente se ha presentado interrupción en la conexión de las máquinas de la organización con el servidor de impresión. Los técnicos han vuelto a instalar el software y a reiniciar el servicio de impresión. Sin embargo, el problema permanece (fuente: http://sf-sonline wordpress.com/2009/03/08/victor-konder/).
	Ocurrió que el hijo del dueño de la organización colocó su memoria USB en el servidor de banco de datos. Ocurrió una parada en el servicio y toda la línea de producción tuvo sus actividades interrumpidas por dos horas. El equipo técnico aún está investigando por qué ocurrió el problema y qué se puede hacer para evitar que se repita.

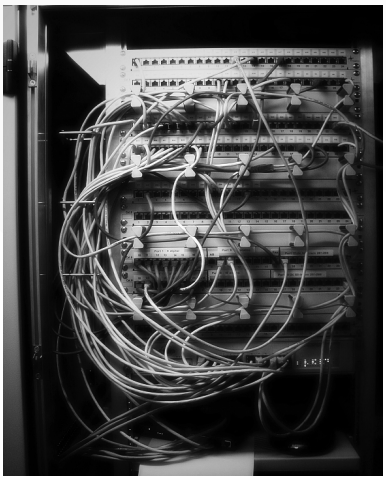
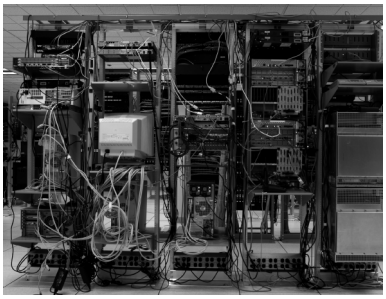
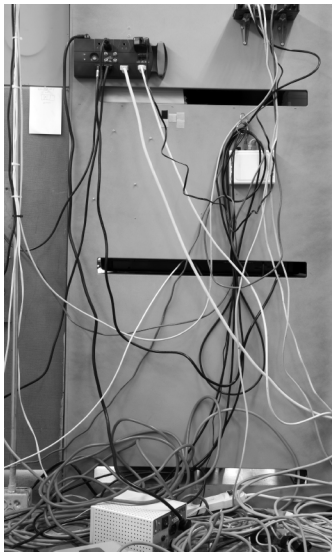
Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	El equipo responsable del link de internet de la organización se sorprendió de la re-inicialización del *router* de la operadora después de haber llamado para el arreglo del mismo y el restablecimiento de la conexión a internet. Al llegar a la sala de equipos se dieron cuenta de que el *rack* estaba abierto.
	Después de la interrupción en la sala de conferencias de la organización durante la reunión entre la dirección y la presidencia, los técnicos de TI (contratistas) fueron accionados para identificar lo que había ocurrido. Los técnicos demoraron cinco horas para contestar a los directivos. Por esta razón se había rescindido su contrato. Y la organización optó por la contratación de otra organización para proporcionar soporte de TI.
	Este enredo de cables perturba el buen funcionamiento y la agilidad en la resolución de problemas. La organización, preocupada con este escenario, contrató a una organización externa para resolver el problema.
	La situación de los equipos de energía y telefonía ha mostrado estado descuidado y los equipos permanecen abiertos. No hay ningún control de acceso a los equipos.

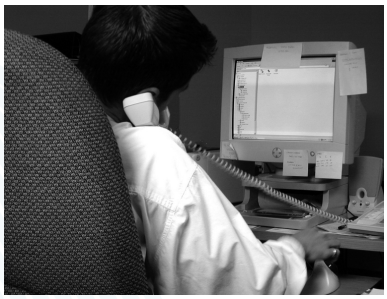
Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	Una vez al llegar a trabajar, los funcionarios se vieron sorprendidos por la caída de parte del techo a causa de las fuertes lluvias que se produjeron. El equipo técnico de redes tuvo serios problemas para resolver la conexión de los equipos de toda la organización para que los mismos pudieran trabajar en red y apoyar el resto de la organización.
	La estructura de la organización fue sacudida por vientos y lluvias fuertes. La red del equipo de soporte del proveedor de Internet estuvo aislada durante la precipitación en la región.
	Se ha producido inestabilidad en la conexión de red del edificio entre los equipos de los diferentes departamentos de la organización y de la sala de servidores, parando todos los servicios a lo largo de un día y provocando la insatisfacción de los usuarios. Está siendo evaluado por expertos técnicos de las TI cuál podría ser la causa de esta inestabilidad.
	El personal de las TI verificó que hay personas que usan el equipo de la organización para juegos electrónicos durante las horas de trabajo, lo que va contra la política de la organización. El administrador del sistema de la organización utiliza su "perfil" para permitir juegos durante el trabajo y pasa parte del día jugando. El jefe de las TI está buscando una manera de educar al administrador para evitar esta práctica durante la jornada laboral.

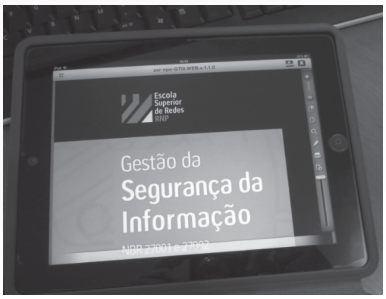
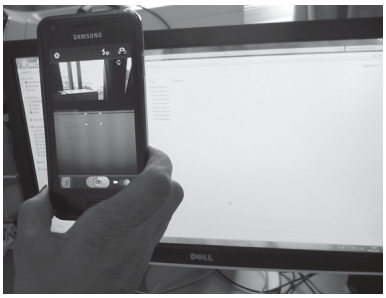
Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	Situación de los cables en el *rack* del almacén.
	Visión del cableado en la parte posterior de los equipos de *datacenter.*
	Una imagen de la filial de la organización.

Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	En la oficina del director están expuestos recordatorios de contraseñas de varios sistemas. Según el director: "La organización no tiene problemas de seguridad. Aquí todo el mundo es digno de confianza."
	Es común encontrar a los empleados utilizando sus *tablets* para acceder a los juegos durante la jornada laboral vía red inalámbrica de la organización.
	Situación encontrada en un *notebook* en uso por un gerente.
	Situación de la documentación de visitantes en la portería donde el sistema de vigilancia y la puerta de seguridad no funcionan hace seis meses.

Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	Un gran número de empleados usa t*ablets y smartphones* para acceder a la red inalámbrica de la organización.
	Depósito de material al lado del depósito de material inflamable.
	Sala de archivo de software y sistemas.
	Se encontró una visitante tomando fotografías de la pantalla de un computador con su celular.

Continuación tabla 18. Ejercicio problemas reportados

Fotografía	Vulnerabilidad
	Infiltración en la sala de servidores en Medellín.
	Infiltración en la sala de servidores en Barranquilla (fuente: http://estadodeminas.lugarcerto.com.br/app/noticia/noticias/2008/12/06/interna_noticias, 28526/sinais-de-infiltracao.shtml).

11.5 Guía de actividades 5

Visión general de la actividad

Después de que equipo tenga las listas de activos, vulnerabilidades y consecuencias, se inicia el trabajo de estimación del riesgo. Aquí, el equipo evalúa la relevancia de los activos y la severidad de las consecuencias, con las actividades necesarias para el "Análisis del riesgo – estimación del riesgo."

La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de gestión del riesgo:

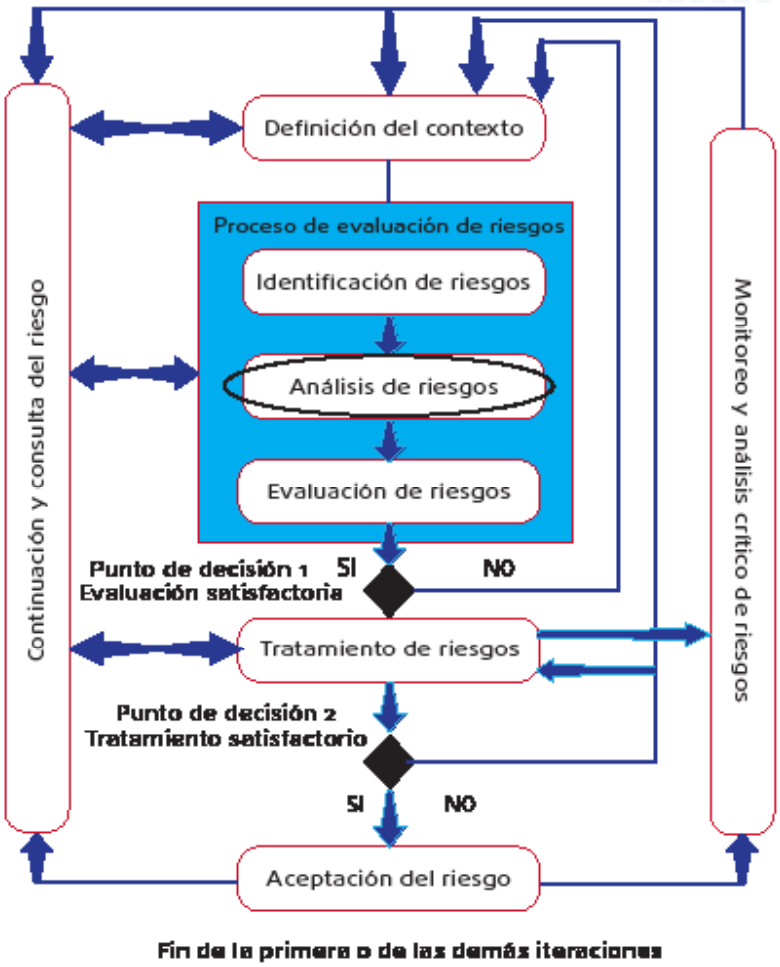


Figura 46. Actividades del proceso de gestión del riesgo. Análisis de riesgos

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo ofrecido y también por la experiencia y conocimientos en la organización.

Para esta actividad el estudiante se debe usar las observaciones sobre la organización KWX.

La secuencia de las actividades será:

1. Lectura de la Sección 8.3.2 y del anexo E de la norma ICONTEC NTC-ISO/IEC 27005.
2. Explicación y demostración de la Tabla 19 y Tabla 20 por el instructor.
3. Ejecución de las actividades propuestas.

En esta guía se encuentran dos tablas:

1. la tabla "Evaluación cualitativa de los activos"
2. la tabla "Evaluación cualitativa de la severidad "

a. Ejercicio de la guía "Evaluación cualitativa de los activos" - Evaluación de la relevancia de los activos

En este ejercicio el equipo de análisis identificará la relevancia de cada activo para los negocios de la organización. Para cada relevancia de cada activo debe ser presentada la evidencia (justificación).

Los criterios de relevancia fueron definidos en la guía de actividades 2 y ahora se aplicarán.

Para el ejercicio, los criterios serán elegidos de una lista de acuerdo a los criterios definidos anteriormente.

Sólo pase a la guía siguiente cuando haya terminado.

Tabla 19. Evaluación cualitativa de los activos

Activos	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia	Justificación/ Evidencias
				Pérdida de integridad	Crítico	

Relevancia de activos
Insignificante
Baja
Significante
Importante
Crítico

b. Actividad de la guía "Evaluación cualitativa de la severidad "- Evaluación de la severidad de las consecuencias.

En esta actividad, el equipo de análisis identificará la severidad de cada consecuencia anteriormente levantada sobre determinado activo y su relevancia para el negocio de la organización.

La respuesta será dada por uno de los niveles del criterio "Severidad de las consecuencias" definido en la guía de actividades 2 en la guía de "Criterios".

Para cada consecuencia, el equipo de análisis definirá la severidad de las consecuencias sobre aquel activo. Para cada severidad de cada consecuencia debe ser presentada la evidencia (justificación).

Para el ejercicio, los criterios serán elegidos de una lista que presentará los criterios definidos anteriormente.

Tabla 20. Evaluación cualitativa de la severidad

Activos	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia	Justificación/ Evidencias
				Pérdida de integridad	Crítico	

Relevancia de activos
Insignificante
Baja
Significante
Importante
Crítico

Sólo pase a la guía siguiente cuando haya terminado.

4. Verificación y corrección por parte del instructor.

Al completar la guía de actividades 5, el equipo de análisis tendrá una lista que contiene los activos, las amenazas que afectan o pueden afectar a cada activo, los controles existentes o con previsión de implementación, las vulnerabilidades que existen en cada activo y las consecuencias en el caso de que estas vulnerabilidades sean explotadas por agentes de amenaza. Ya han determinado aún la relevancia de cada activo para los negocios de la organización y la severidad de las consecuencias.

11.6 Guía de actividades 6

Visión general de la actividad

En esta guía, serán realizadas las actividades necesarias para el "Análisis del riesgo - probabilidad y la estimación del riesgo."

La siguiente figura muestra la ubicación de estas actividades en el proceso de la gestión del riesgo:

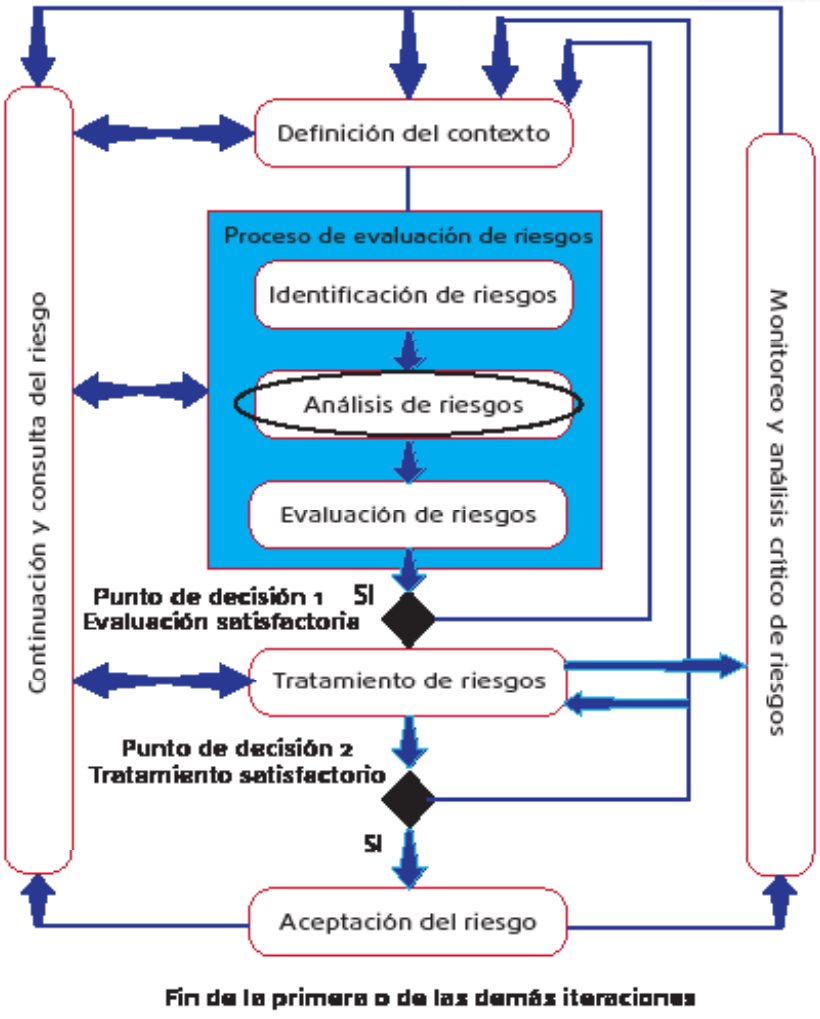


Figura 47. Actividades en el proceso de gestión del riesgo. Probabilidad y la estimación del riesgo.

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo suministrado además de la experiencia en su organización.

Para esta actividad el estudiante se debe valer de las observaciones de la organización KWX.

La secuencia de las actividades será:

1. Lectura de las secciones 8.3.2, 8.3.3 y 8.3.4 de la norma ICONTEC NTC ISO/IEC 27005;
2. Explicación y demostración de la Tabla 21 a la Tabla 23 por el instructor;
3. Ejecución de las actividades propuestas;

En esta guía se encuentran las siguientes tablas:

1. la tabla "Evaluación Cualitativa Probabilidad
2. la tabla "Estimativa"
3. la tabla "Res. Estimativa Cualitativa"

a. Ejercicio de la guía "Evaluación cualitativa de la probabilidad"- Evaluación de la probabilidad

En este ejercicio el equipo de análisis identificará y definirá la probabilidad de que las vulnerabilidades sean explotadas y sus respectivas consecuencias.

Con una visión más amplia de las vulnerabilidades y consecuencias, el equipo definirá la probabilidad de ocurrencia de estos eventos. Los criterios de probabilidades se definen durante la segunda guía de actividades y ahora serán aplicados.

Para cada vulnerabilidad el equipo analizará y definirá su probabilidad. Se debe presentar la evidencia (justificación) para cada posibilidad de vulnerabilidad de los activos.

Para el ejercicio, los criterios de probabilidad serán elegidos de acuerdo a como han sido definidos anteriormente.

Tabla 21. Evaluación cualitativa de la probabilidad

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Probabilidad	Justificación/Evidencias

Probabilidad
Frecuente
Probable
Ocasional
Remoto
Improbable

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicio de la guía "Estimación" - Definición de las estimaciones (pesos).

En este ejercicio, el equipo de análisis ya conocerá todo el ambiente, sus activos, vulnerabilidades y la probabilidad de ocurrencia, y así definirá los pesos para la definición y cálculo de riesgo.

La inserción de pesos en cada criterio tiene por objetivo facilitar el cálculo de riesgos y por lo tanto permitir que sean ordenados por criticidad.

Los criterios fueron definidos en la guía de actividades 2. Ahora se hará sólo la inserción de los pesos en cada criterio. Tenga en cuenta que en esta actividad no será hecho ningún cambio en los criterios definidos anteriormente. En caso de que se identifique la necesidad de cambiar los criterios durante el proceso de gestión del riesgo, será necesario regresar a la actividad de criterios y rehacerla, revisando todo el trabajo desde allí.

Para el ejercicio, la guía "Estimación" presenta los criterios definidos anteriormente, multiplicados por la columna "Peso". En esta columna se colocará el peso definido por el equipo de análisis de riesgo a partir de su visión de la organización. La planilla ya presenta los pesos con valor "0", y el equipo tiene que reemplazarlos por los valores que considere válidos. Por ejemplo:

- 1, 2, 3, 4 y 5;
- 1, 3, 5, 7, y 9;
- 1, 2, 3, 6 y 10;
- 1, 2, 4, 6 y 8.

Estos pesos pueden ser cambiados para que puedan representar a la realidad de la organización. El equipo establece estos pesos por su experiencia con la organización. Cada valor de peso debe tener una justificación de su valor.

Además de los criterios de riesgo, aparece la puntuación para cada criterio, calculada de forma automática a partir de los pesos dados por el equipo, así como también la asignación de prioridades de tratamiento del riesgo asumidos por el equipo.

Tabla 22. Definición de las estimaciones

Criterios de probabilidad		
Nivel	**Definición**	**Peso**
Frecuente	Ha ocurrido por lo menos una vez al mes	4
Probable	Puede ocurrir cada 6 meses o menos. En los últimos seis meses ya se ha producido	3
Ocasional	En el último año se han producido al menos una vez	2
Remoto	En los últimos cinco años se ha producido al menos tres veces	1
Improbable	Nunca ocurrió	0

Relevancia Activos		
Nivel	**Definición**	**Peso**
Insignificante	De acuerdo con la organización	1
Baja	De acuerdo con la organización	2
Media	De acuerdo con la organización	3
Alta	De acuerdo con la organización	4
Elevada	De acuerdo con la organización	5

Severidad de las consecuencias		
Nivel	**Definición**	**Peso**
Insignificante	Los acontecimientos no afectan al negocio o no causan interrupción durante más de cinco minutos	1
Baja	De acuerdo con la organización	2
Media	De acuerdo con la organización	3
Alta	De acuerdo con la organización	4
Elevada	De acuerdo con la organización	5

Impacto			
Nivel	**Definición**	**Peso**	**Cálculo**
Insignificante	De acuerdo con la organización	1	5
Baja	De acuerdo con la organización	2	10
Significativo	De acuerdo con la organización	3	15
Importante	Afectan la imagen de la organización y causan interrupción de 12 horas al negocio. La compañía hace deja de funcionar/ producir durante 12 horas	4	20
Desastre	De acuerdo con la organización	5	25

Criterios de riesgo					
Nivel	Definición	Estimación de riesgos			
					Prioridad
Externo	La organización interrumpe totalmente sus servicios por más de 48 horas, parando para realizar y producir servicios, afectando su imagen pública de manera significativa. Financieros: altas pérdidas, demandas judiciales.	81	100		1
Alto	De acuerdo con la organización	49	80		2
Medio	De acuerdo con la organización	19	48		3
Bajo	De acuerdo con la organización	5	18		4
Irrelevante	De acuerdo con la organización	1	4		5

Sólo pase a la guía siguiente cuando haya terminado.

c. Actividad de la guía "Res. estimación cualitativa "- Resultados de las estimación.

En esta actividad, el equipo de análisis estudiará el resultado de las estimaciones para identificar si realmente cumplen las necesidades del negocio de la organización.

El equipo debe analizar los resultados en detalle.

Para el ejercicio, analice cada resultado y presente su justificación informando si cumple o no los requisitos de la organización. Para facilitar la comprensión, regrese a la actividad anterior y cambie los pesos, comprobando lo que sucede con los resultados.

» En su visión de analista de riesgos, ¿cuál resultado cumple mejor a los requerimientos del negocio?

» Analice todos los resultados de la estimación, y en caso de duda consulte al instructor.

Tabla 23. Estimación cualitativa

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	IMPACTO = RELEVANCIA DE ACTIVOS * SEVERIDAD	Probabilidad	Justificación/Evidencias

Sólo pase a la guía siguiente cuando haya terminado.

4. Verificación y corrección por parte del instructor.

Al completar la "Guía de actividades 6", el equipo de análisis tendrá una visión general de los resultados de los análisis de riesgo, donde se puede identificar el impacto de cada consecuencia si las vulnerabilidades son explotadas por el agente de amenaza.

11.7 Guía de actividades 7

Visión general de la actividad

En esta actividad serán realizados los procesos necesarios para el "Análisis del riesgo - evaluación del riesgo" en una evaluación cualitativa.

La siguiente figura muestra la ubicación de estas actividades en el proceso de la gestión del riesgo:

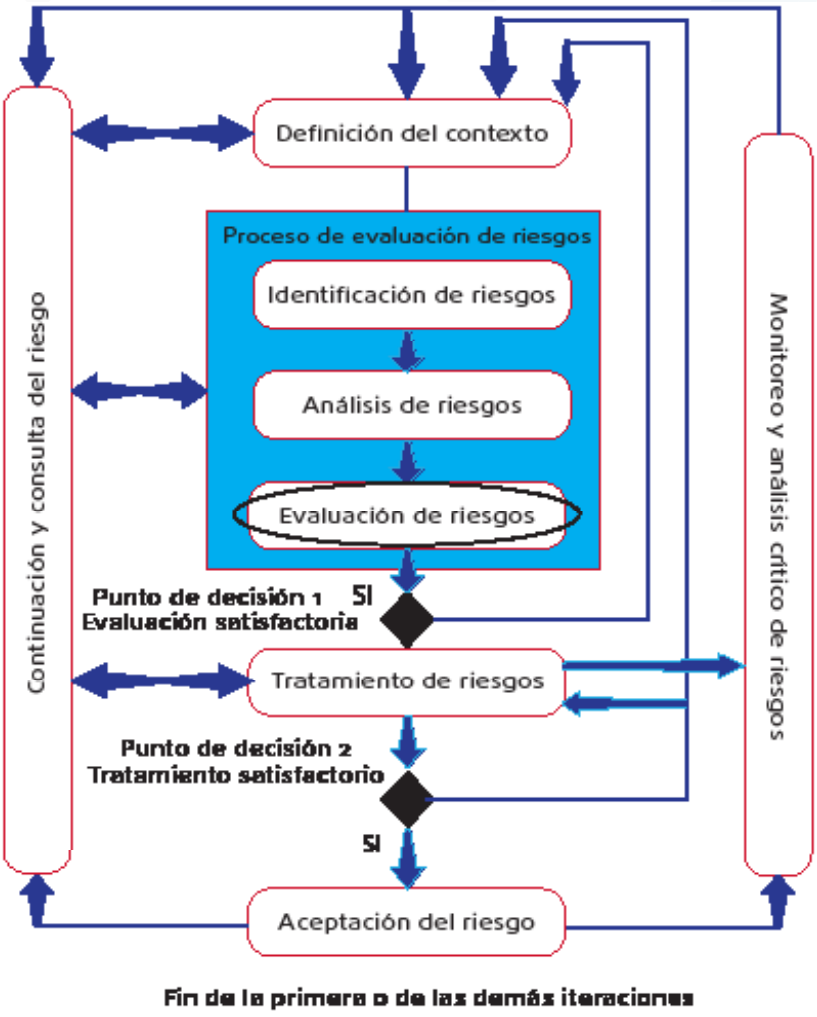


Figura 48. Actividades en el proceso de gestión del riesgo. Evaluación cualitativa.

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC ISO/IEC 27005, del material de apoyo suministrado y por la experiencia en su organización.

Para esta actividad el estudiante se debe valer de las observaciones de la organización KWX.

La secuencia de las actividades será:

1. Lectura de la sección 8.4 de la norma ICONTEC NTC ISO/IEC 27005.
2. Explicación y demostración de la Tabla 24 y Tabla 25 por el instructor.
3. Ejecución de las actividades propuestas.

Se encuentran las siguientes tablas:

1. la tabla "Calcular el riesgo"
2. la tabla "Evaluar el Riesgo"

a. Ejercicio de la guía "calcular riesgo" - cálculo del riesgo.

En esta actividad el equipo de análisis realizará el cálculo del riesgo.

Con las actividades previas ya realizadas, el trabajo en esta actividad es de supervisión y análisis de los resultados con la aplicación de los criterios. Para efectos de este ejercicio, el equipo debe analizar cuidadosamente los resultados y ver si hay acuerdo con los resultados del riesgo presentados.

» Para facilitar la comprensión, vuelva a las actividades de las guías 5 y 6 y cambie sus respuestas, observando lo que ocurre con los resultados en esta guía 7.
Comente sus impresiones sobre los resultados.

» En este análisis de riesgo, ¿cuál es la cantidad de riesgos "extremos"? Y, ¿cuáles son los riesgos considerados "Altos" y "bajos"?

Tabla 24. Cálculo del riesgo

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicios de la guía "Evaluar el riesgo" - evaluación del riesgo.

Después de que el equipo de análisis haya calculado el riesgo y con el conocimiento de todo el ambiente y de sus problemas, se debe hacer una evaluación del riesgo y de sus resultados, definiendo la prioridad de mitigación de estos riesgos.

Para efectos del ejercicio, la prioridad será elegida de la lista definida en la guía "Estimativa" de la sección 6. Para cada prioridad definida el equipo de análisis debe presentar la evidencia (justificación).

Tabla 25. Evaluación del riesgo

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto	Evaluación de riesgos Prioridad	Justificación

Sólo pase a la guía siguiente cuando haya terminado.

4. Verificación y corrección por parte del instructor.

Al completar la "Guía de actividades 7", el equipo de análisis estará con un listado de los activos y riesgos para cada vulnerabilidad. Este listado permite la definición de los riesgos más grandes, colocándolos en orden de prioridad y estableciendo los controles que deben ser empleados para tratarlos.

11.8 Guía de actividades 8

Visión general de la actividad

En esta actividad, serán realizadas las actividades necesarias para el "Análisis de riesgo - tratamiento y aceptación del riesgo."

La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de la gestión del riesgo.

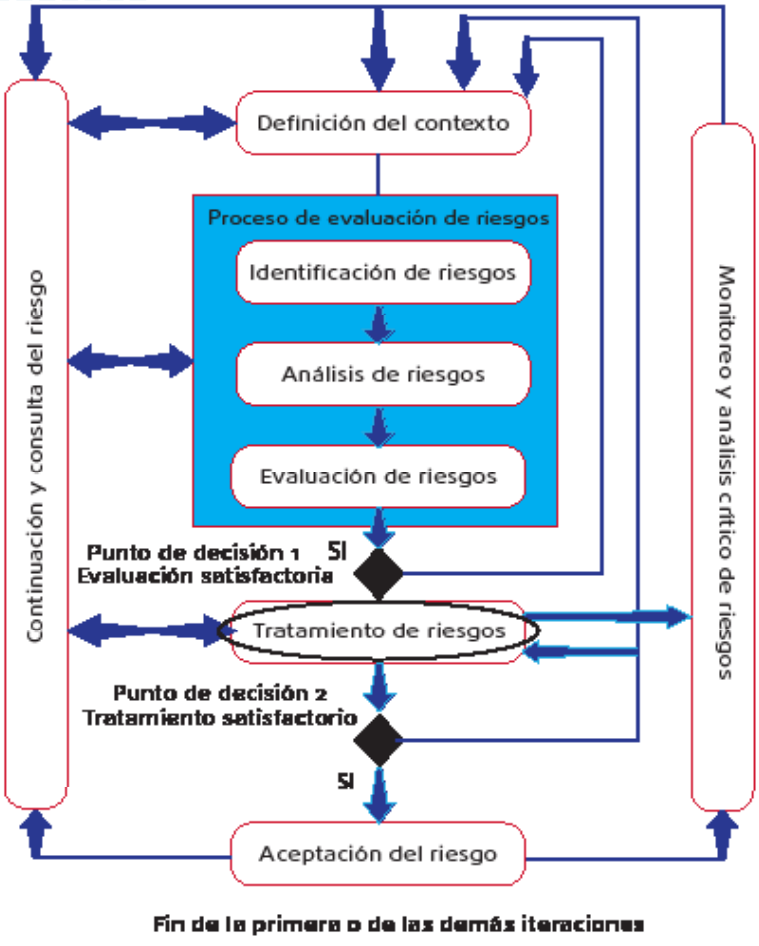


Figura 49. Actividades en el proceso de gestión del riesgo. Tratamiento de riesgos.

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo brindado y también por la experiencia y conocimientos en su organización.

Para esta actividad el estudiante debe valer de las observaciones sobre la organización KWX.

La secuencia de las actividades será:

1. Lectura de las sesiones 9 y 10 de la norma ICONTEC NTC-ISO/IEC 27005;
2. Explicación y demostración de la Tabla 27 a la Tabla 29 por el instructor;
3. Ejecución de las actividades propuestas;

En esta actividad se encuentran cuatro tablas:

1. la tabla "Tratamiento"
2. la tabla "Controles del Plan"
3. la tabla "Riesgos residuales"
4. la tabla "Aceptación del Riesgo"

a. Ejercicio de la guía "Tratamiento" - Definición de tratamiento de los riesgos.

En este ejercicio el equipo de análisis definirá la forma de tratamiento que cierto riesgo deberá recibir. Para esto, el equipo de riesgo elegirá una de las formas de tratamiento:

- Modificación del riesgo;
- Retención del riesgo;
- Acción para evitar el riesgo;
- Compartir el riesgo.

Para cada forma de tratamiento de los riesgos debe ser presentada la evidencia (justificación).

Tabla 26. Definición de tratamiento de los riesgos

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto	Evaluación de riesgos Prioridad	Tratamiento	Justificación

Tratamiento
Modificación de riesgo
Riesgo de retención
Medidas para evitar el riesgo
Distribución de riesgos

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicio de la guía "Controles del plan" - Definición de los controles
En este ejercicio, el equipo definirá los controles que se deben implementar para mitigar los riesgos encontrados. Con su experiencia y conocimiento del ambiente, el equipo seleccionará los mejores controles que realmente va a ser eficaz y eficientes en el tratamiento del riesgo. Estos controles forman parte del plan de tratamiento del riesgo, que es uno de los resultados de un análisis del riesgo.

La pregunta clave aquí es: ¿Qué controles se deben aplicar sobre las vulnerabilidades para mitigar los riesgos provocados por ellas?

Para el ejercicio, deberán ser identificados dos controles que permiten la mitigación del riesgo en el menor tiempo posible. Para fines de aprendizaje, se recomienda comenzar con los controles de la norma NTC ISO/IEC 27002.

El equipo de análisis en este ejercicio debe analizar cada vulnerabilidad y sus riesgos y decidir los mejores controles, presentando sus justificaciones.

Tabla 27. Definición de controles

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto	Evaluación de riesgos Prioridad	Tratamiento	Control 1	Control 2	Justificación

Sólo pase a la guía siguiente cuando haya terminado.

c. Ejercicio de la guía "Riesgos residuales" - Levantamiento de los riesgos residuales.

En este ejercicio, el equipo de análisis identificará y definirá los riesgos residuales después de la aplicación de los controles. Esta es una actividad de vital importancia, dado que les permitirá comprobar si los riesgos realmente disminuirán y alcanzarán hasta el nivel aceptable por la organización.

Además de verificar los riesgos residuales, el equipo deberá, si el riesgo aún se mantiene por encima del nivel aceptable, proponer nuevos controles o aún controles de compensación, de manera que el nivel de riesgo se reduzca el máximo posible y el más cercano del aceptable. Si esto no es posible, se debe realizar un nuevo ciclo de análisis de riesgo. La respuesta será dada por uno de los niveles del criterio "severidad de las consecuencias", definido en la Sección 2, en la guía "Criterios".

Para el ejercicio, se llenarán las siguientes columnas:

- "Existen riesgos residuales?" - para cada riesgo y los controles implementados el equipo deberá responder (sí o no);
- ."¿Cuáles? Describa "- el equipo deberá informar los riesgos y vulnerabilidades que aún no fueron tratados (riesgos residuales);
- "Justificación / Evidencia" - el equipo deberá presentar las evidencias del riesgo residual;
- "Nueva serenidad" – caso existan riesgos residuales, el equipo deberá analizarlas y establecer nueva severidad, seleccionando de la lista similar de la Sesión 5. Al elegir el ítem de la lista, automáticamente aparece el peso de esta severidad en la siguiente columna;
- "Nueva probabilidad" - después de diligenciar la columna de la nueva severidad, deberá ser diligenciada la nueva probabilidad, seleccionando de la lista similar al realizado en la Sección 6. Al elegir de la lista, aparece automáticamente el peso de esta probabilidad en la siguiente columna.

Tabla 28. Levantamiento de los riesgos residuales

Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto	Evaluación de riesgos Prioridad	Tratamiento	Control 1	Control 2	Hay Riesgo Residual?	¿Qué? Describa	Justificación	Nueva Severidad	Nueva probabilidad

Al diligenciar estas columnas aparecerá el nuevo valor del riesgo residual. Caso aún esté por encima del nivel aceptable aparecerá un mensaje de error al lado.

Sólo pase a la guía siguiente cuando haya terminado.

d. Ejercicios de la guía "Aceptación del Riesgo" - Aceptación de los riesgos.

En esta actividad, el equipo de análisis y la organización, como partes interesadas, conducirán las actividades necesarias para la aceptación de los riesgos.

Esta aceptación es un documento formal que establece que el riesgo será aceptado, una justificación para eso y el responsable por la toma de decisión. Por lo general, los que tienen el poder para tomar esta decisión es parte de la alta dirección. Esta aceptación se realizará únicamente a los riesgos que aún se encuentran por encima del nivel aceptable.

Para el ejercicio se llenarán tres columnas:

1. "Decisión" - ¿cuál la decisión de aceptación del riesgo? Una elección debe hacerse a partir de una lista de opciones.
2. "Justificación" - justificación para la toma de decisión.
3. "Responsable" - nombre de la persona encargada de la toma de decisión.

Caso el riesgo no sea aceptado la celda debe ser dejada en blanco.

Tabla 29. Aceptación del riesgo

														Riesgos residuales			Aceptación del riesgo		
Activo	Amenaza	Control existente	Vulnerabilidades encontradas	Consecuencias	Relevancia de activo	Severidad/Consecuencias	Impacto	Probabilidad	Riesgo = Probabilidad x Impacto	Evaluación de riesgos Prioridad	Tratamiento	Control 1	Control 2	¿Hay Riesgo Residual?	¿Qué? Describa	El riesgo residual es...	Decisión	Justificación	Responsable

Sólo pase a la guía siguiente cuando haya terminado.

4. Verificación y corrección por parte del instructor.

Al concluir la "Guía de actividades 8", el equipo de análisis habrá prácticamente completado el análisis de riesgo. En esta etapa se habrán recorrido todas las actividades de la gestión del riesgo, con pleno conocimiento de los activos críticos, sus amenazas y vulnerabilidades, el tratamiento y los controles que necesitan ser implementados y, una vez implementado, identificar los riesgos residuales que aún puedan existir. Observe la figura al inicio de cada guía de actividades y verifique la ejecución de todas las etapas del proceso de gestión del riesgo.

11.9 Guía de actividades 9

Visión general de la actividad

En esta actividad, serán realizadas las actividades necesarias para el "análisis de riesgo - comunicación de los riesgos."

La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de la gestión del riesgo:

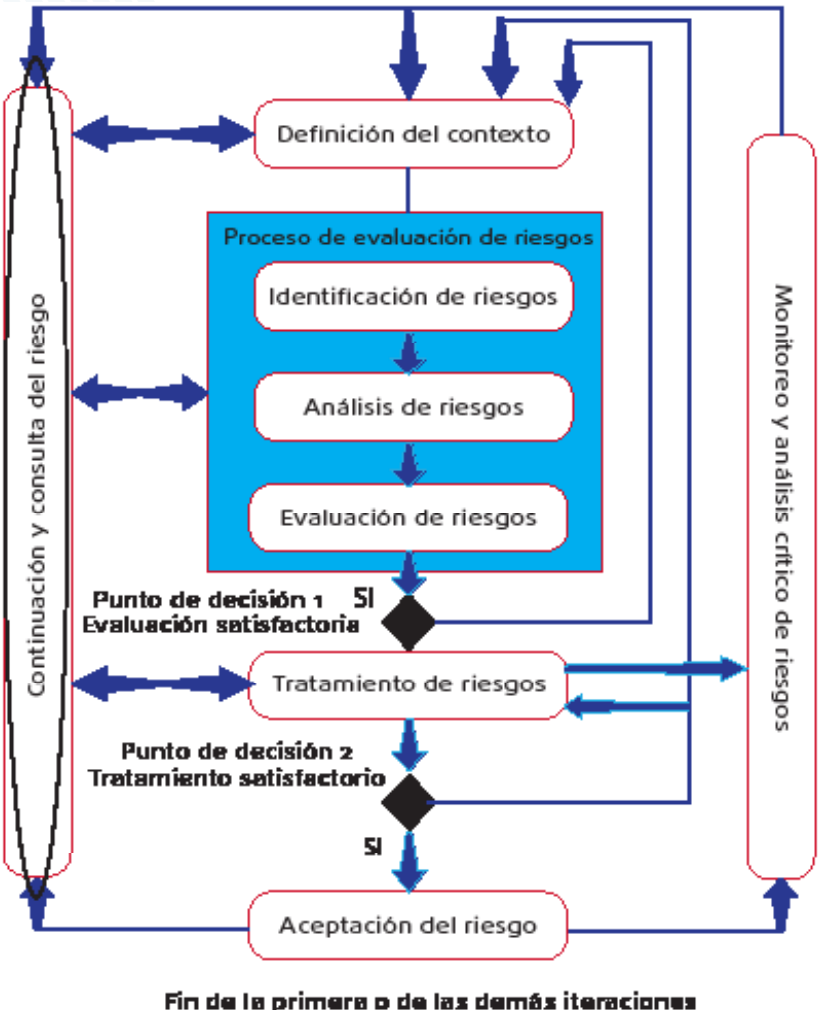


Figura 50. Actividades en el proceso de gestión del riesgo. Comunicación del riesgo.

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo suministrado y también por la experiencia y vivencia en su organización.

Para esta actividad el alumno se debe valer de las observaciones de la organización KWX.

La secuencia de las actividades será:

1. Lectura de la sección 11 de la norma ICONTEC NTC ISO/IEC 27005;
2. Explicación y demostración de la Tabla 30 por el instructor;
3. Ejecución de las actividades propuestas;

a. Actividad de la guía "Comunicación del riesgo" – Comunicación del riesgo.

En esta actividad, el equipo de análisis realizará las actividades necesarias para la comunicación durante el proceso de gestión del riesgo. Esta actividad se lleva a cabo durante toda la gestión del riesgo. En cada actividad realizada el equipo deberá realizar la comunicación de una manera planificada.

Para efectos del ejercicio, el equipo de análisis de riesgo contestará una serie de preguntas que tienen como objetivo mostrar una cadena de comunicaciones durante toda la gestión del riesgo en la organización, para así permitir una perfecta comprensión de esta importante actividad. La comunicación permitirá orientar y concientizar sobre la importancia de la gestión del riesgo.

Tabla 30. Comunicación del riesgo

Comunicación del riesgo	Justificación
¿Cómo debe hacerse la comunicación de riesgos en la organización?	
¿Quién es responsable de la comunicación de riesgos en el análisis del equipo?	
¿Quién es responsable de la comunicación de riesgos en la organización?	
¿Cuál es el equipo de procedimiento para identificar un alto riesgo con la gravedad?	
¿Cuál es el equipo de procedimiento para descubrir nuevas amenazas que han surgido en determinado activo?	

Continuación tabla 30. Comunicación del riesgo

Comunicación del riesgo	Justificación
En medio del proceso de revisión del equipo fue informado de que la topología de la red va a cambiar. ¿Cuál es el procedimiento de comunicación del equipo de este cambio?	
Presenta el diagrama de flujo de la comunicación que trabajará durante este proyecto.	
¿Cómo es la comunicación de los resultados a la agencia que solicitó el análisis?	
¿En qué momento inicia la comunicación en la gestión del riesgo?	
¿Cuándo el equipo de análisis de riesgo se comunicará considerado vulnerabilidades críticas identificadas en la sesión 3?	
Teniendo en cuenta este ejercicio, en que momento (s) se celebraron efectivamente "comunicaciones" para los interesados en el proyecto?	
Teniendo en cuenta este año, ¿quién debe asistir a la reunión final para presentar los resultados?	
¿Qué temas serán presentados por el equipo de análisis de riesgo, mientras que comunican los resultados finales?	
Ejemplifica con la actividad un evento desencadenante que requieren comunicación inmediata. ¿Cómo se formalizará la comunicación? Justificar.	
En ese momento termina la comunicación dentro de la gestión del riesgo? Un ejemplo de este ejercicio.	

Sólo pase a la guía siguiente cuando haya terminado.

4. Verificación y corrección por parte del instructor.

Al concluir la "Guía de actividades 9", el equipo de análisis tendrá el conocimiento y la comprensión de los procedimientos adoptados para realizar la comunicación durante toda la gestión del riesgo.

11.10 Guía de actividades 10

Visión general de la actividad

En esta actividad, serán realizadas las actividades necesarias para el "Análisis de riesgo – monitoreo de los riesgos."

La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de la gestión del riesgo:

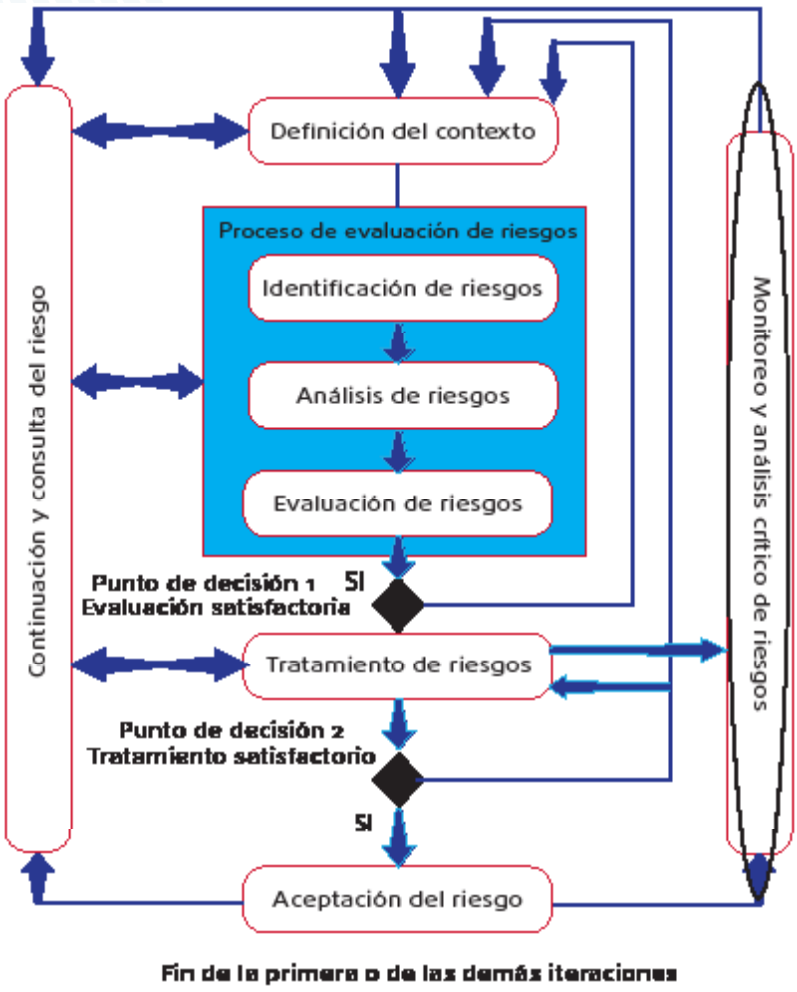


Figura 51. Actividades del proceso de gestión del riesgo. Monitoreo de los riesgos.

La realización de esta actividad debe ir acompañada de la lectura de la norma ICONTEC NTC-ISO/IEC 27005, del material de apoyo suministrado y también por la experiencia en su organización.

Para esta actividad el alumno se debe valer de las observaciones de la organización KWX.

La secuencia de las actividades será:

1. Lectura de la sección 12 de la norma ICONTEC NTC- ISO/IEC 27005;
2. Explicación y demostración de la Tabla 31 y Tabla 32 por el instructor;
3. Ejecución de las actividades propuestas;

En la guía se encuentra dos tablas:

1. la tabla "Monitoreo de Riesgos"
2. la tabla "Monitoreo, mejoría, proceso"

a. Ejercicio de la guía "Monitoreo de Riesgos" - Monitoreo y análisis crítico del riesgo de seguridad de la información.

En este ejercicio, el equipo de análisis realizará las actividades necesarias para el monitoreo y análisis crítico del riesgo. Estas actividades en la realidad son desarrolladas desde la primera actividad del proceso de gestión del riesgo.

Esta actividad tiene como objetivo el monitoreo y el análisis crítico de los riesgos encontrados. ¿El equipo está encontrando los riesgos? ¿Está pudiendo observar algo?.

Para el ejercicio, el equipo de análisis de riesgo contestará a una serie de preguntas que tienen como objetivo mostrar un proceso lógico de monitoreo y análisis crítico de riesgos durante toda la gestión del riesgo, para permitir una perfecta comprensión de esta importante actividad de la organización. El monitoreo y el análisis crítico de riesgos guiará y mejorarán la ejecución de los trabajos del equipo de análisis de la gestión del riesgo.

Tabla 31. Monitoreo de riesgos

Monitoreo de riesgos	Justificación
¿Cómo funciona el monitoreo de equipo de análisis?	
¿Cuál es el procedimiento para identificar una nueva información de eventos de seguridad?	
¿Qué se controla durante la realización de análisis de riesgos?	
¿Quién es responsable de la vigilancia?	
¿En qué momento se realiza el seguimiento?	
¿Cuál es el propósito de la finalización de la revisión en este trabajo?	
¿Cómo es el análisis crítico en este trabajo?	
¿Cuál es la relación entre el monitoreo y el análisis crítico?	
¿Cuál es el procedimiento para el examen?	
¿Qué se hará para identificar un problema durante la revisión?	
¿Cuál es el procedimiento para el seguimiento y análisis crítico, para descubrir nuevas amenazas? ¿Y para los nuevos activos?	
Teniendo en cuenta el ejercicio de análisis del riesgo, ¿las actividades requieren una supervisión bastante estricta?	
A qué medida el equipo de análisis debe hacer un análisis crítico de la aceptación del riesgo?	
¿Cómo debe ser llevado a cabo para identificar el análisis crítico de las vulnerabilidades?	

Sólo pase a la guía siguiente cuando haya terminado.

b. Ejercicio de la guía "Monitoreo, mejoría, proceso" - Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo.

En este ejercicio, el equipo de análisis llevó a cabo en conjunto con la organización las actividades necesarias para el monitoreo, análisis crítico y mejora del proceso de gestión del riesgo. Estas actividades se desarrollan con el objetivo de identificar si la gestión del riesgo es eficiente, eficaz y satisfactoria a los requisitos del negocio.

Esta actividad tiene como objetivo hacer el monitoreo del proceso de gestión del riesgo y el análisis crítico a la mejora continua de la gestión del riesgo. ¿El proceso de gestión del riesgo está funcionando? ¿Qué se necesita para mejorar el proceso de gestión del riesgo?

Para el ejercicio, el equipo de análisis de riesgos contestará una serie de preguntas que tienen como objetivo mostrar un proceso lógico de monitoreo, análisis crítica y mejora del proceso de gestión del riesgo en la organización, buscando la mejora continua de los procesos y de las actividades que conforman.

Tabla 32. Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo

Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo	Justificación
¿Cómo es el seguimiento del proceso de gestión del riesgo para la organización?	
¿Qué parte del equipo de análisis hace el seguimiento del proceso de gestión del riesgo?	
¿Cómo es el análisis crítico realizado por la organización? ¿En qué momento se realiza?	
¿Qué parte del equipo realiza el análisis crítico del proceso de gestión del riesgo?	
¿Qué hace la organización con los resultados de la vigilancia? Y de análisis crítico?	

Continuación tabla 32. Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo

Monitoreo, análisis crítico y mejora del proceso de gestión del riesgo	Justificación
¿Cómo la organización lleva a cabo la mejora del proceso de gestión del riesgo?	
¿Qué parte del equipo de análisis se dedica a mejorar el proceso de gestión del riesgo?	
Conocer la organización para integrar el equipo de análisis, ¿qué recomendaciones vas a hacer para mejorar el proceso?	
¿Cuándo se debe hacer un nuevo análisis de riesgos?	
En el caso del ejercicio, ¿la organización debe acompañar a la obra para mejorar el proceso de gestión del riesgo?	
En el caso del ejercicio, para completar su trabajo, ¿qué observaciones tiene sobre el seguimiento del proceso de gestión del riesgo?	
En el caso del ejercicio, para completar su trabajo, ¿cuáles son sus observaciones con respecto a la mejora continua del proceso de gestión del riesgo?	

4. Comprobación y corrección por parte del instructor.

Al concluir la "Guía de actividades 10", el equipo de análisis habrá completado todo un ciclo de la gestión del riesgo. Los pasos a seguir son los siguientes:

- Elaborar un informe con los resultados (activos, amenazas, vulnerabilidades, consecuencias, impactos y riesgos priorizados);
- Hacer un plan de tratamiento que contiene los controles que deben ser implementados para la mitigación de los riesgos.

Es importante que todo trabajo se realice basado en las normas de seguridad de la información que sirve de base para la gestión de seguridad de la información.

Conclusión

Visión general de la gestión del riesgo

En este curso se observaron todos los aspectos de la gestión del riesgo, de acuerdo con la norma ICONTEC NTC-ISO/IEC 27005. La siguiente figura muestra gráficamente la ubicación de estas actividades en el proceso de gestión del riesgo.

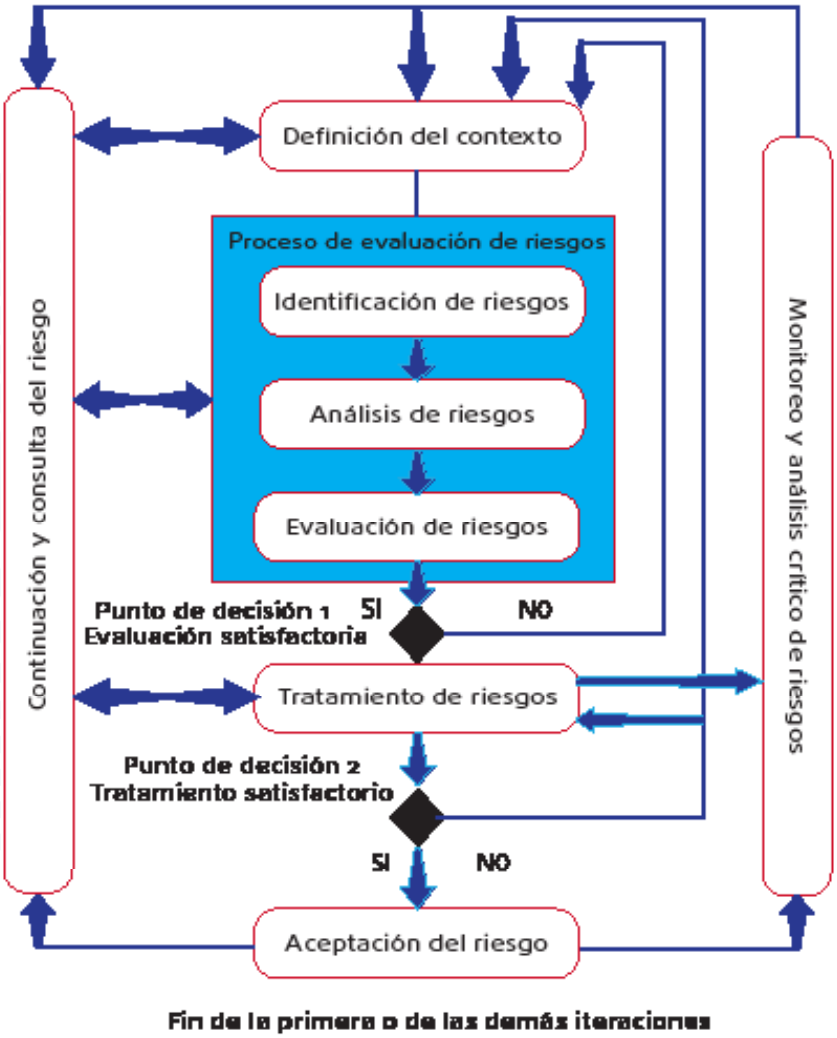


Figura 52. Actividades en el proceso de gestión del riesgo.

Los objetivos de proporcionar conocimientos sobre la gestión del riesgo y suministrar una herramienta para la realización de la gestión del riesgo se detallaron y se practican en cada sesión de aprendizaje de este curso. Es importante saber que cuando se hace un primer ciclo de la gestión del riesgo, este proceso se vuelve cíclico y continuo.

La gestión del riesgo es un proceso que siempre va a traer beneficios a la organización. La mejora de las condiciones de seguridad de la información pasa necesariamente por el conocimiento de las debilidades y

vulnerabilidades que pueden ser explotadas para que las amenazas se materialicen. Y, sin duda, la mejor manera de hacer esto es a través de la gestión del riesgo.

Bibliografía

CERIAS. The Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu/ (acesso em julho de 2013).

Cert.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil: http://www.cert.br/links/ (acesso em julho de 2013).

DE CICCO, Francesco; FANTAZZINI, Mario Luiz. Tecnologias consagradas de gestão de riscos. São Paulo: Risk Tecnologia Editora, 2003.

Enterprise Risk Management: Past, Present and Future: http://www.casact.

org/education/erm/2004/handouts/kloman.pdf (acesso em julho de 2013).

Interdisciplinary Risk Management:,
http://www.riskinfo.com/rmr/rmrjun05.htm (acesso em julho de 2013).

Marcos Sêmola – website Gestão de Riscos da Informação: http://www.semola.com.br/conceitos.html (acesso em julho de 2013).

NBR Guia 73 – Gestão de riscos – Vocabulário

NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança –

Código de prática para a gestão da segurança da informação.

NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

NBR ISO/IEC 31000 – Gestão de riscos – Princípios e diretrizes.
PELTIER, Thomas R. Information Security Risk Analysis. CRC Press, 2005.

SANS – The Cyber Security Risks:
http://www.sans.org/top-cyber-security-risks/?ref=top20 (acesso em julho de 2013).

Security Focus – Vulnerabilities: http://www.securityfocus.com/ (acesso em julho de 2013).

WESTERMAN, George; HUNTER, Richard. O risco de TI. Harvard Business

School Press, 2008.

ICONTEC ISO GTC 137 Gestión del riesgo – Vocabulario

ICONTEC NTC ISO/IEC 27001:2006

ICONTEC NTC ISO/IEC 27002:2005

ICONTEC NTC ISO/IEC 27005:2008 Tecnología de la Información – Técnicas de Seguridad – Gestión del riesgo de seguridad de la información

ICONTEC NTC ISO 31000 Gestión del riesgo – Principios y directrices

Lista de figuras

Lista de tablas

Planeación y Gestión Estratégica de las TI

Versión ESR-Colombia
Escuela Superior de Redes, ESR - Colombia

Se publicó en el mes de julio de 2014,
Publicado por RENATA,
Universidad Nacional de Colombia,
Facultad de Ingeniería
Bogotá D. C., Colombia.
En su diagramación se utilizaron caracteres DaxlinePro

Esta versión está adaptada para Ecuador gracias a CEDIA.

www.cedia.org.ec

GESTIÓN DEL RIESGO DE LAS TI NTC 27005

Calle La Condamine 12-109 "Casa Rivera"
Teléfono (+593) 7 405 1000 Ext. 4220
info@cedia.org.ec • Cuenca - Ecuador
/FundacionCEDIA @FundacionCEDIA