

VALORACIÓN DE RIESGOS



VALORACIÓN DE RIESGOS

Todas las actividades que se efectúan o interactúan dentro de la organización, implican riesgos. El riesgo es un evento incierto sobre los activos de la organización. El riesgo, se debe identificar, valorar para establecer sus consecuencias en la organización y su probabilidad de ocurrencia.

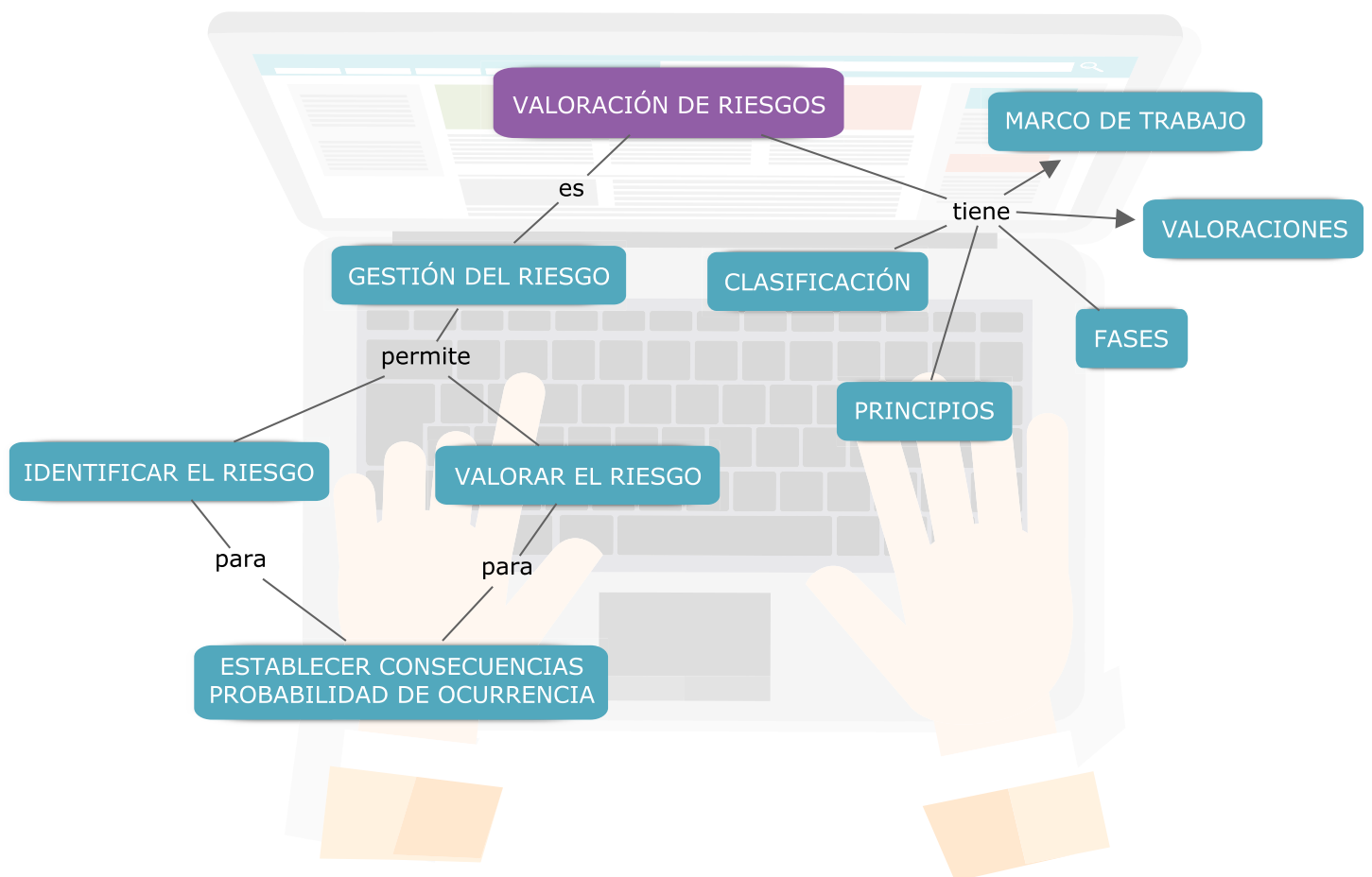
Se debe establecer un orden de prioridad para poder tratar los riesgos que puedan presentarse y priorizar las acciones que permitan reducir la ocurrencia de los mismos, puesto que siempre estarán presentes. Y es la alta dirección, la que debe tomar decisiones sobre los riesgos encontrados en la organización y emprender las acciones necesarias para el manejo de los riesgos que puedan afectar negativamente el logro de los objetivos propuestos en la organización, de esta manera permite la gestión del riesgo.

La gestión del riesgo se puede aplicar a toda la organización, en todas sus áreas o dependencias, en cualquier momento. Así como a sus funciones, sus proyectos y a cualquier tipo de actividad.

ESTRUCTURA DE CONTENIDOS

Introducción	2
Mapa Conceptual	4
1. ¿QUÉ ES RIESGO?	5
2. PRINCIPIOS DE GESTIÓN DEL RIESGO (ISO 31000- FRETT, N. 2013)	6
3. CLASIFICACIÓN DEL RIESGO	7
4. FASES PARA LA VALORACIÓN DEL RIESGO	9
4.1 Identificación de riesgos	9
4.2 Identificación de controles	9
5. VALORACIÓN DEL RIESGO	10
5.1 Riesgo inherente	12
5.2 Riesgo marginal	13
6. MARCO DE TRABAJO	14
Bibliografía	16
Glosario	17
Control de Documentos	18
Creative Commons y Marca Registrada	18

MAPA CONCEPTUAL







1. ¿QUÉ ES RIESGO?

Un riesgo en seguridad de la información, es un evento incierto el cual, puede producir efectos positivos o negativos sobre los activos de la organización.

“El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado” (Vilches, M.).

Dentro de las características de un riesgo se pueden mencionar:

-  **Situacionales:** Varían de una situación a otra.
-  **Interdependiente:** Al tratar un riesgo puede provocar otro riesgo o aumentar su impacto.
-  **Magnitud:** Pérdida o daño posible.
-  **Tiempo:** Ocurre en un cierto periodo.



2. PRINCIPIOS DE GESTIÓN DEL RIESGO (ISO 31000- FRETT, N. 2013)

La Norma ISO 31000 establece que todo proceso de gestión de riesgo debe:



Crear y proteger el valor: Contribuye a la consecución de objetivos así como a la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.



Estar incorporada en todos los procesos: No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.



Ser parte del proceso para la toma de decisiones: La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas de acción.



Ser usada para tratar con la incertidumbre: La gestión de riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.



Ser estructurada, sistemática, y oportuna: Contribuye a la eficiencia y consecuentemente, a la obtención de resultados fiables.



Basada en la mejor información disponible: Los inputs del proceso de gestión de riesgos están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.



Adaptarse a su entorno: Hecha a su medida, alineada con el contexto externo e interno de la organización y con su perfil de riesgo.



Considerar factores humanos y culturales: Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna que pueda facilitar o dificultar la consecución de los objetivos de la organización.



Ser transparente, inclusiva, y relevante: La apropiada y oportuna participación de los grupos de interés y, en particular, de los responsables a todos los niveles, deben asegurar que la gestión del riesgo permanece relevante y actualizada.



Dinámica, sensible al cambio, e iterativa: La organización debe velar para que la gestión de riesgos detecte y responda a los cambios de la empresa. Conocer como ocurren los acontecimientos externos e internos, cambio del contexto, nuevos riesgos que surgen y otros que desaparecen.



Facilitar la mejora continua de la organización: Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

3. CLASIFICACIÓN DEL RIESGO

Las fuentes de riesgo son factores o circunstancias del trabajo que pueden generar uno o varios riesgos aisladamente o por su combinación.

Ejemplo: Ambiente de Procesamiento: el riesgo se genera con el acceso indebido a los programas y datos que pueden estar almacenados en ese ambiente.

Los riesgos se clasifican en:



Riesgos internos: Sus fuentes se dan dentro de la organización.



Riesgos externos: Sus fuentes se dan fuera de la organización.



Riesgo de Negocios: Es el riesgo de los negocios estratégicos de la empresa y de sus procesos claves. En otras palabras es un riesgo crítico de la empresa.



Riesgo Inherente: Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por la organización.



Riesgo de Auditoría: Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.



Riesgo de Control: Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.



Riesgo de Cumplimiento: Se asocia con la capacidad de la empresa para cumplir con los requisitos regulativos, legales, contractuales, de ética pública, democracia y participación, servicio a la comunidad, interacción con el ciudadano, respeto a los derechos, a la individualidad, la equidad y la igualdad.



Riesgo Estratégico: Se asocia con la forma en que se administra la organización. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la organización, la cual busca la vigilancia de la conducta de los servidores públicos, defender el orden jurídico y los derechos fundamentales.



Riesgo Operativo: Comprende tanto el riesgo en sistemas como operativos, provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.



Riesgo Financiero: Se relaciona con las exposiciones financieras de la empresa. El manejo del riesgo financiero incluye actividades de tesorería, presupuesto, contabilidad y reportes financieros, entre otros.



Riesgo de Tecnología: Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.



Riesgo Laboral: Conjunto de normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos, de las enfermedades y los accidentes que puedan ocurrirles con ocasión o como consecuencia del trabajo que desarrollan.

4. FASES PARA LA VALORACIÓN DEL RIESGO

Para realizar la valoración del riesgo, se debe identificar los activos de información de la empresa, y determinar el valor de éstos. Con estos elementos, se procede a identificar el grado de exposición e impacto que puede generar a la organización, si los activos son alterados de alguna forma.

Para llevar a cabo el proceso de valoración del riesgo, se deben tener en cuenta las fases de identificación de riesgos y la identificación de controles.

4.1 IDENTIFICACIÓN DE RIESGOS

En esta fase, se determina para cada uno de los activos de la organización, las amenazas a las que está expuesto el activo y se da prioridad al activo en riesgo (en confidencialidad, integridad, disponibilidad) que tenga mayor valor para la organización.



4.2 IDENTIFICACIÓN DE CONTROLES

En esta fase, se define, diseña y se realiza seguimiento a los controles que permitan tratar y evaluar los riesgos que se deban implementar para mitigar el impacto de las amenazas identificadas en la primera fase (ver tabla 1).



Los controles tienen una escala cualitativa: Muy Adecuado, Adecuado, Moderado, Débil, Muy Débil.

Los cuales se cuantifican en:

Eficiencia: del 10% al 90%

Marginalidad: entre 0.1 y 0.9

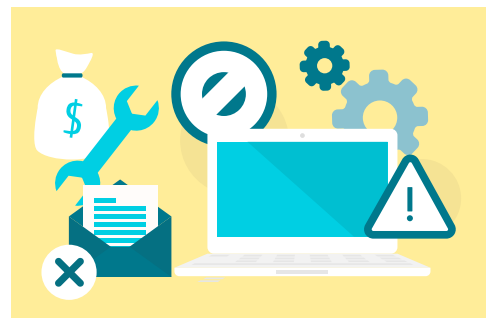


Tabla1. Evaluación del control del riesgo. (Caviedes, Prado, Muñoz. (s.f.)).






Cualificación	Consideración	Eficiencia	Marginalidad
Muy Adecuado	El control establecido tiene un diseño fuerte, es automático y se comprueba su efectividad.	90%	0.1
Adecuado	El control establecido tiene un diseño fuerte, no es automático, se comprueba su efectividad.	70%	0.3
Moderado	El control establecido tiene un diseño fuerte, no es automático, no se comprueba su efectividad.	50%	0.5
Débil	El control establecido no tiene un diseño fuerte, no es automático, pero se comprueba su efectividad.	30%	0.7
Muy Débil	El control establecido no tiene un diseño fuerte, no es automático, no se comprueba su efectividad.	10%	0.9

Para llevar a cabo la valoración del riesgo en cuanto a su eficacia, se debe considerar la fortaleza del control que se establece para mitigar el riesgo, el grado de automatización y, si se tienen o no registros de la eficiencia del control establecido.

5. VALORACIÓN DEL RIESGO

En esta fase, se debe de considerar la probabilidad de que la amenaza que se identifica ocurra, e impacte el activo.

Para determinar la probabilidad de que ocurra la amenaza se establecen las siguientes frecuencias:






-  Nada Frecuente.
-  Poco Frecuente.
-  Normal.
-  Frecuente.
-  Muy Frecuente.

A los cuales se les asigna un valor cualitativo entre 0.2 y 1. (ver tabla 2).

Tabla 2. Probabilidad de que ocurra una amenaza.(Caviedes, Prado, Muñoz. (s. f.))

Valor	Frecuencia	Ocurrencia
0.2	Nada frecuente	No ha sucedido.
0.4	Poco frecuente	Sucede cada 10 años.
0.6	Normal	Sucede una vez al año.
0.8	Frecuente	Sucede mensualmente.
1	Muy frecuente	Sucede diariamente.

Para determinar el impacto del activo en cuanto a la probabilidad de ocurrencia, se determina la siguiente degradación:

-  Insignificante.
-  Menor.
-  Moderado.
-  Mayor.
-  Catastrófico.

A los cuales se les asigna un valor entre 0.2 y 1 (Ver Tabla 3).

Tabla 3. Estimación de impacto. (Caviedes, Prado, Muñoz. (s.f.))

Valor	Degradación	Ocurrencia
0.2	Insignificante	El activo no sufre daños que impidan su operación.
0.4	Menor	El activo sufre daños y puede continuar operando.
0.6	Moderado	El activo sufre daños y su operación es restringida.
0.8	Mayor	El activo sufre daños que impiden su operación y puede recuperar dentro del tiempo tolerable para la operación.
1	Catastrófico	El activo sufre daños irreparables y la operación se altera considerablemente.

Al identificar la probabilidad de que ocurra una amenaza (tabla 2) y la estimación de impacto (tabla 3), se procede a calcular el riesgo inherente y el riesgo marginal.

5.1 RIESGO INHERENTE

Son aquellos riesgos propios de la materia y/o componentes de ésta. Se entiende que una materia por su naturaleza tiene riesgos que surgen por diversas fuentes, como los errores, irregularidades o fallas que pudieran ser importantes en forma individual o en conjunto con otros riesgos. Los riesgos inherentes a la materia pueden tener o no controles elaborados por la dirección para mitigar su probabilidad o su impacto.

Los riesgos inherentes a la materia bajo análisis pueden ser relativos al entorno, ambiente interno, procesos, información, etc.:



Riesgo de Crédito: Exposición a una pérdida real o el costo de oportunidad como consecuencia del incumplimiento de pago de una persona natural o jurídica.



Riesgo Financiero: Ocurrencia de un imprevisto por variaciones o cambios en la economía local o internacional que podría afectar los descalces de caja o posiciones asumidas por inversiones y su liquidez, como asimismo los descalces globales de activos.



Riesgo Operacional: Se define como el riesgo de pérdida debido a la inadecuación o fallas en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos (fraudes, daños activos materiales, fallas en procesos, etc.) Incluye riesgos legales y normativos.



Riesgo de Tecnología de la Información: Agrupa todos los riesgos asociados con la autorización, integridad, y exactitud de las transacciones según se ingresan, se procesan, se resumen y se informan en los sistemas computacionales de una organización.



Riesgo Calidad de Servicio y Transparencia de la Información: Se puede presentar por la disminución de la calidad y accesibilidad de los trámites y servicios, y la accesibilidad a la información.

Para el cálculo del riesgo inherente se utiliza la siguiente fórmula:

$$\text{riesgo_inherente} = \text{frecuencia} * \text{degradación}.$$

Dónde:

Frecuencia: Es el valor obtenido de la probabilidad de que ocurra una amenaza (tabla 2).

Degradación: Es el valor obtenido de la estimación de impacto (tabla 3).



5.2 RIESGO MARGINAL

Es el límite o margen que pueden tener los riesgos dentro de la organización.

Para el cálculo del riesgo marginal se utiliza la siguiente fórmula:

$$\text{riesgo_marginal} = \text{riesgo_inherente} * \text{marginalidad}$$

Dónde:

Riesgo_inherente: Es calculado en la fórmula anterior

Marginalidad: Es el valor obtenido en la evaluación de control del riesgo (tabla 1)



Al obtener los resultados, se deberá establecer una respuesta a los riesgos identificados para cada uno de los activos de información de la organización, a los cuales se les realizará seguimiento en cuanto a eficiencia y respuesta.



Gráfica. Metodología para la valoración del riesgo. (Guzmán. (s.f.))



6. MARCO DE TRABAJO

El marco de trabajo o marco de referencia o la estructura para la gestión del riesgo menciona que la introducción de la gestión del riesgo y el aseguramiento de su eficacia continua, requieren un compromiso fuerte y sostenido de la dirección de la organización, así como el establecimiento de una planificación estratégica y rigurosa para conseguir el compromiso a todos los niveles.





BIBLIOGRAFÍA

Alexander, A. (2013). Análisis y evaluación del riesgo de información: un caso en la Banca. Aplicación del ISO 27001:2005. Consultado el 12 de julio de 2015 en:

http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

Emaza. (2010). Los 10 tipos de activos en la Seguridad de la Información ¿Qué son y cómo valorarlos? Artículo web. Consultado el 12 de julio de 2015, en: <http://www.seguridadinformacion.net/los-10-tipos-de-activos-en-la-seguridad-de-la-informacion-que-son-y-como-valorarlos/>

Gómez, Á. (2007). Enciclopedia de la seguridad informática. Alfaomega grupo editor, México.

Icontec. (2011). Gestión del riesgo. Principios y directrices. NTC/ISO 31000:2011

GLOSARIO

Activo: Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una organización, institución o individuo, y que se reflejan en su contabilidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Propietario del riesgo Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad: Ausencia de riesgo o también a la confianza en algo o alguien.



Control de documento Construcción Objeto de Aprendizaje Valoración de riesgos	
Desarrollador de contenido Experto temático	Juan José Botello Castellanos Jenny Marisol Henao García Yuly Paulín Sáenz Agudelo
Asesor pedagógico	Juan José Botello Castellanos
Producción Multimedia	Julio César Orduz Tarazona Victor Hugo Tabares Carreño
Programador	Adriana Rocío Pérez Rojas
Líder línea de producción	Santiago Lozada Garcés

