Uruguay Presidencia | agesic

Proceso de Evaluación y Monitoreo de Riesgos

Identificar – Analizar – Evaluar - Comunicar

Importante: El presente documento es para trabajo interno; no para su difusión fuera del ámbito de Agesic.

SEGURIDAD DE LA INFORMACIÓN
Versión 1.

Este documento ha sido elaborado por AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El procedimiento que se presenta en este documento es únicamente para realizar análisis y evaluaciones de los riesgos y no determina la manera exacta en que se puede o debe realizar dicha medición por cada organización, sin embargo, se puede tomar de modelo para el cumplimiento del marco de ciberseguridad.

Proceso de Evaluación y Monitoreo de Riesgos

Objetivo

Establecer un procedimiento general para identificar, analizar, evaluar y comunicar los riesgos internos y externos a los cuales la organización se puede encontrar expuesta.

Alcance

El proceso define las acciones mínimas a considerar cuando se identifica un riesgo para la organización, y que por ello requiera ser incluido en los procedimientos de análisis y tratamiento en caso de corresponder. Establece un método de medición semi-cuantitativo entre la probabilidad de materialización del riesgo y el impacto probable sobre la organización. Finalmente, establece acciones de comunicación de los riesgos a las partes interesadas, a los efectos de lograr un tratamiento adecuado.

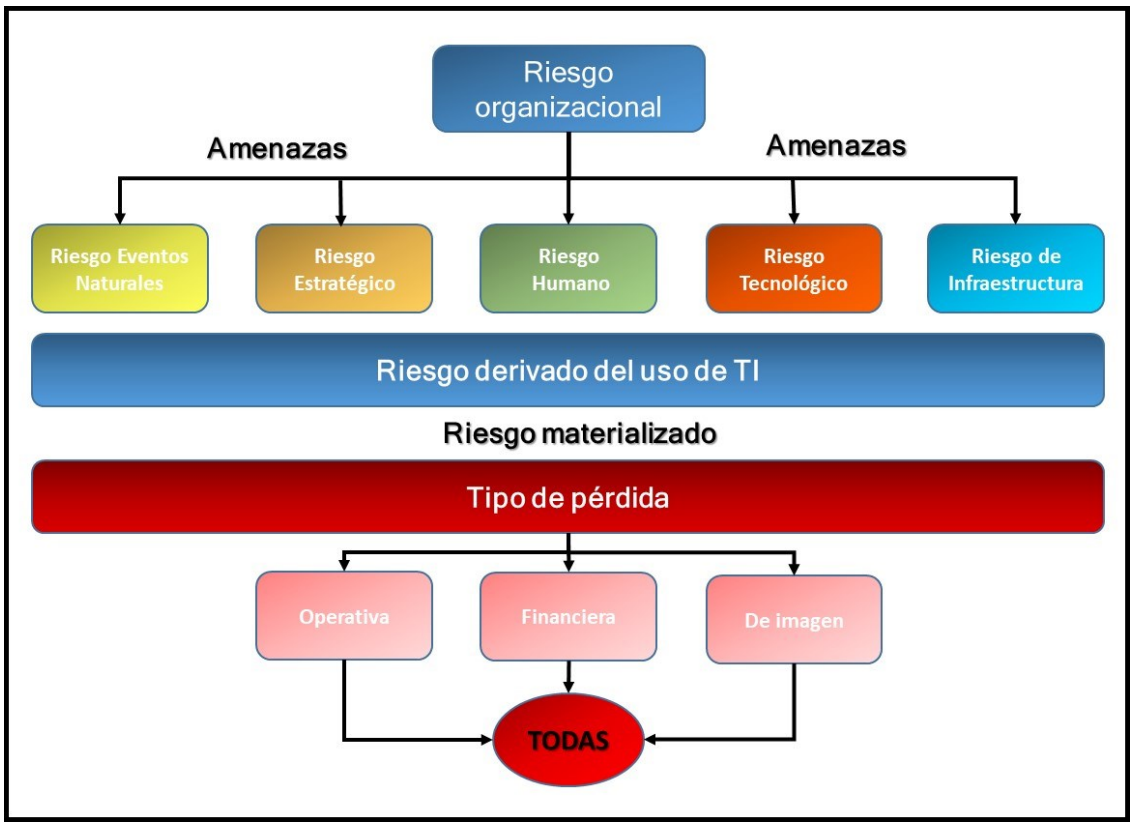
Responsabilidades

- Responsable de seguridad de la información: debe velar por el desarrollo, cumplimiento y tratamiento de los riesgos de la organización.
- La Organización: encargada de difundir, fomentar y apoyar el programa de gestión de riesgos a todo el personal y en asistir a cada área involucrada en aquellos procesos que puedan verse afectados.

Descripción

La metodología se presenta en cuatro pasos a ejecutar durante el proceso de la evaluación del riesgo: Identificar, Analizar, Evaluar y Comunicar.

Medir el riesgo en base al eje tecnológico es fundamental, ya que en general la mayoría de los procesos se apoyan en sistemas, subsistemas o activos que están conectados a elementos tecnológicos y pueden ser un punto de falla que pudieran provocar pérdidas de índole operativa, financiera y/o de imagen pública.

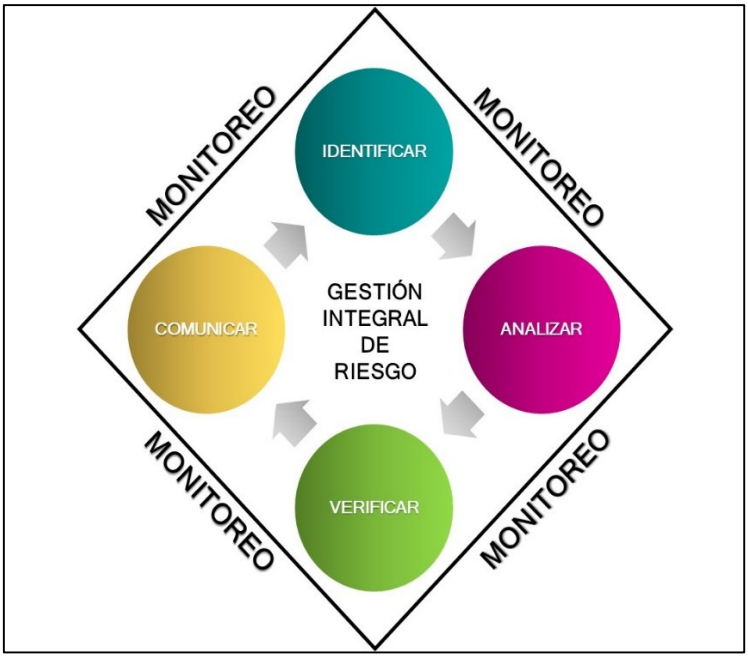


Premisas del riesgo

- El análisis de los riesgos en general surge como un proyecto interno de la organización, el cual puede deberse a requerimientos de la normativa aplicable o debido a necesidades internas.
- Resulta clave identificar los procesos y actividades por área para detectar los riesgos asociados.
- En general, partir de los riesgos derivados del uso de la TI facilita la identificación de riesgos en otros procesos o tareas.
- El riesgo no debe ser evaluado en forma independiente por un área, es un trabajo de equipo en el que participan referentes de las áreas relevantes y del que surgen acciones consensuadas y adecuadas a las necesidades de la organización.

- El tratamiento de los riesgos no implica su eliminación por completo. En general, se pueden establecer controles que disminuyan la probabilidad y/o impacto, aunque puede ocurrir que un determinado riesgo no pueda ser mitigado debido a factores culturales, económicos o tecnológicos. Los riesgos que se aceptan, aunque no estén de acuerdo a la tolerancia de riesgos de la organización deben estar aceptados formalmente.

Pasos a seguir para el análisis y evaluación del riesgo



I. Identificar

Requiere que se identifiquen:

- Todos los sistemas con la que cada área de la organización ejecuta sus tareas.
- Las áreas de la organización que hacen uso del sistema.
- Todo activo de información asociado a un proceso crítico de la organización.

Es necesario considerar el origen del riesgo, qué amenaza explota y a qué activos afecta. En base a ello, se debe puntuar la probabilidad de ocurrencia y el impacto en caso que ocurra, en base a la experiencia organizacional o datos de la industria.

II. Analizar

Requiere que se contesten cuatro premisas:

- Qué puede pasar: Se analiza desde las perspectivas de la situación actual a qué riesgos se puede estar expuesto.
- Cuándo puede pasar: Se analiza la probabilidad que tiene un riesgo de materializarse en un determinado momento.
- Cómo puede pasar: Se analiza la posible causa que puede favorecer la materialización del riesgo.
- Tipo de pérdida: Se analiza dependiendo de la causa cuál es el posible impacto a la organización en torno a tres puntos importantes como ser pérdida financiera, operativa, de imagen pública o todas las anteriores.

El análisis del riesgo es un trabajo continuo de un grupo conformado por miembros de las diferentes áreas o al menos diferentes miradas sobre los activos de información a evaluar. La identificación y el análisis de los riesgos es un procedimiento que se mejora en identificaciones sucesivas, inicialmente será normal partir del peor caso de forma tal de cubrir todos los efectos sobre la organización en caso que el riesgo se materialice.

En este punto, se trabaja sobre los riesgos ya identificados, analizando los controles existentes sobre los riesgos, determinando cuán efectivo es el control existente en la mitigación de los riesgos.

III. Verificar

La verificación de los riesgos implica comparar el nivel del riesgo obtenido contra el nivel de riesgo que la organización está dispuesta a asumir.

El objetivo final de esta etapa es evaluar la toma de acciones en base a los riesgos cuyos niveles resulten inaceptables para la organización.

IV. Comunicar

La efectiva comunicación de los riesgos es un aspecto esencial para que cada área conozca los riesgos a los que la organización está expuesta y las acciones que se han tomado para tratar los mismos.

- Es importante comunicar todos los pasos a seguir durante la evaluación de riesgo a todas las áreas y partes interesadas (dentro y fuera de la organización).
- La presentación de los resultados obtenidos no debe omitir los riesgos que por su naturaleza o complejidad no pueden ser mitigados o transferidos. El mapa de calor de riesgos es una representación gráfica de la probabilidad e impacto.
- La comunicación en tiempo y forma fomentará la colaboración para la evaluación de los riesgos de forma continua y proporcionará un mayor entendimiento entre las áreas y partes interesadas en poder trabajar sobre aquellos riesgos que puedan tener un mayor impacto en la organización.

V. Monitoreo constante

Un aspecto esencial de cualquier sistema de gestión integral de riesgos es el monitoreo continuo, para incluir riesgos que pudieran ser omitidos en una identificación anterior, o que cambios en procesos internos o el contexto externo de la organización ameriten una revaluación total o parcial de los riesgos presentes en el inventario. El análisis y la evaluación continua de los riesgos redundarán en una organización más resiliente.

Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en el procedimiento e incumpliendo con la política de seguridad de la información, la Dirección del Organismo podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.