M-SGI-005
Metodología de Análisis de riesgos

Responsables

Elaboró:	Líder del Sistema de Gestión Integral
Revisó:	Gerente de Cumplimiento y Mejora continua
Aprobó:	Dirección General

Control de versiones

Versión	Fecha	Descripción del cambio
1	07/02/19	Emisión inicial.
2	27/05/19	Ajustes en el alcance del diagrama de la metodología de riesgos.
3	07/06/19	Se realizan modificaciones en la metodología de acuerdo con los hallazgos identificados en la auditoría externa.
4	13/07/20	Actualización de logo de acuerdo con la nueva imagen corporativa.
5	13/07/20	Se incluye política derivado de la atención de NC.
6	19/08/22	Actualización de formato, e implementación del SGCN ISO 22301.

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

Organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias internas y externas que hacen incierto saber si se lograran los objetivos. La incidencia de esta incertidumbre tiene sobre la consecución de los objetivos de una organización y constituye el "riesgo".

Todas las actividades de una organización implican riesgos. Las organizaciones gestionan el riesgo identificándolo, analizándolo y evaluando después si el riesgo se debería modificar mediante un tratamiento que satisfaga sus criterios de riesgo. A lo largo de este proceso, las organizaciones comunican y consultan a las partes interesadas, realizando seguimiento, revisando el riesgo y los controles que lo modifican para asegurar que no es necesario un tratamiento adicional del riesgo.

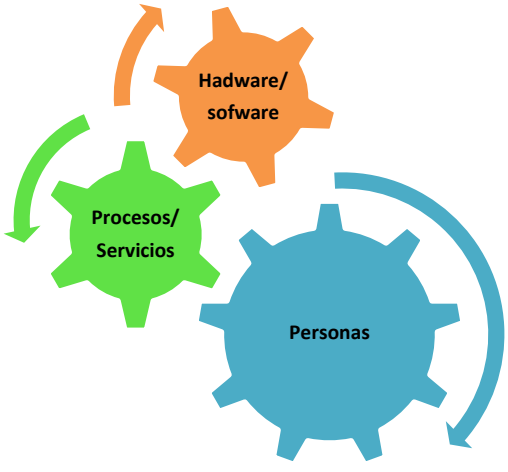
La gestión de riesgos se puede aplicar a la totalidad de una organización, a todas sus áreas y niveles principales, en todo momento, así como a las funciones, los proyectos y las actividades específicas.

Un análisis de riesgos es un proceso para estimar las afectaciones de los activos de la organización tales como: personal, proveedores, clientes, infraestructura, tecnología, documentación, etc., los cuales estén relacionados con la gestión de la calidad del producto y/o servicios brindados.

El análisis facilita la identificación y evaluación de los riesgos, mediante un análisis detallado en cada uno de los procesos establecidos en la organización, con la finalidad de tomar medidas adecuadas para aceptarlo, mitigarlo, eliminarlo, evitarlo o transferirlo; mostrando a su vez un balance al analizar el impacto con relación al costo que implican las soluciones propuestas.

2. Alcance

Esta metodología deberá ser aplicada a los activos, procesos y servicios incluidos dentro del alcance definido para el Sistema de Gestión Integral.



3. Definiciones

Riesgo: efecto de la incertidumbre sobre la concesión de los objetivos.

Nota1: un efecto es una desviación, positiva o negativa respecto a lo previsto. Puede ser positivo, negativo o ambos.
Nota2: los objetivos pueden tener diferentes aspectos (tales como financieros, de salud, seguridad o ambientales) y se pueden aplicar diferentes niveles (tales como nivel estratégico, nivel de un proyecto, de un proceso o de una organización completa)
Nota3: con frecuencia, el riesgo se caracteriza por referencia a un suceso potencial y a sus consecuencias, o una combinación de ambas
Nota4: con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad
Nota5: la incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de sus probabilidades

Riesgo positivo: Es una oportunidad identificada, la cual puede potencializarse por la organización.

Gestión de riesgo: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Pensamiento basado en riesgos: Permite a la organización determinar los factores que podrían causar en los procesos del SGI desviaciones en los resultados planificados, para poner en marcha controles preventivos para minimizar los efectos negativos y maximizar el uso de las oportunidades que surjan.

Probabilidad: posibilidad de que algún hecho se produzca.

Impacto: magnitud de un riesgo o combinación de riesgos**,** expresados en términos.

Activo. Cualquier elemento que sea considerado como valioso para la organización.

Aceptación del riesgo. Decisión tomada por la dirección general de aceptar el riesgo y asumir sus consecuencias.

Calidad: Grado en el que un conjunto de características inherentes cumple con los requisitos.

Evaluación de riesgo. Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

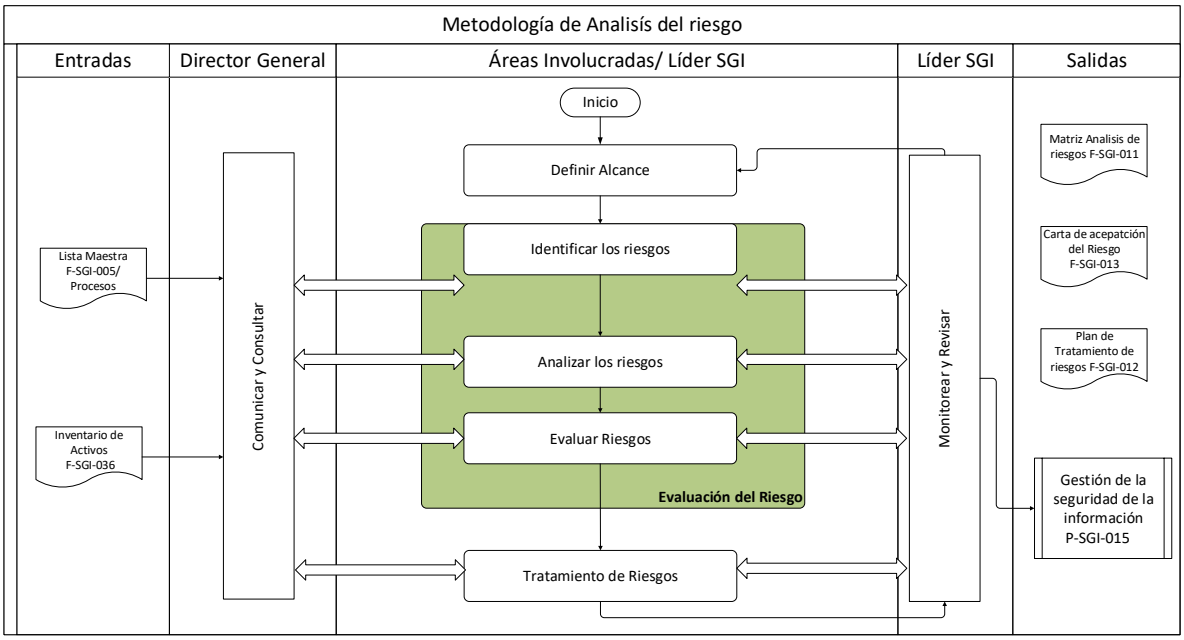
Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Satisfacción del cliente: Percepción del cliente sobre el grado en que se han cumplido sus requisitos.

Tratamiento de riesgo. Implementación de acciones para modificar el riesgo identificado (positivo/negativo).

4. Descripción del manual

4. Diagrama de Análisis de Riesgos



5. Responsabilidades

Dirección General:

- Es el encargado de aprobar este procedimiento.
- Responsable de determinar cuál es el nivel de riesgo aceptable para cada ejecución del análisis y evaluación de riesgos, documentándolo en la Matriz de Análisis de Riesgos.
- Garantizar que el análisis y evaluación de riesgos se lleve a cabo al menos una vez al año, o cuando ocurran cambios importantes en las áreas incluidas en el alcance del SGI (de procesos, tecnología, proveedor, ubicación, nuevos proyectos, etc.) que afecten directamente a los activos de información, procesos y a la operación, así como también cuando sea un requerimiento legal, regulatorio o contractual
- Aprobar el plan de tratamiento de riesgos aceptando los riesgos residuales en el sistema Tabantaj o mediante la carta de aceptación del Riesgo F-SGI-013 (en caso de indisponibilidad de la herramienta), o reunión de revisión de riesgos.

Líder del SGI / Gerente de Mejora continua

- Responsable de revisar y actualizar esta metodología mínima una vez al año, o si ocurren cambios que impacten de manera considerable la calidad, seguridad de la información, la continuidad, y los procesos o la entrega del servicio.
- Coordinar y facilitar la realización del análisis y evaluación de riesgos.
- Presentar los resultados del análisis, evaluación de riesgos, los cuales incluyen el riesgo residual propuesto, a la Dirección General para su aprobación, una vez aprobados se comunicarán a las áreas correspondientes los resultados obtenidos.
- Presentar el Plan de Tratamiento de Riesgos a la Dirección General para su aprobación.
- Presentar los resultados en el Sistema Tabantaj o en la Matriz de análisis de riesgos (F-SGI-011) y el Plan de tratamiento de riesgos (F-SGI-012).
- Llevar a cabo la validación del plan de tratamiento de riesgos, para garantizar la inclusión de todos los identificados en la matriz de análisis de riesgos.

Personal de Silent4business

- Son responsables de participar en el ejercicio del análisis de riesgos
- Aprobar el Plan de Tratamiento de riesgos aceptando los riesgos residuales en Tabantaj, o mediante la carta de aceptación del riesgo (F-SGI-013) o en sesión de presentación de resultados.

6. Descripción de Metodología

A) Definir el alcance

La definición del análisis y evaluación de riesgos es una aproximación metódica para definir el alcance de los escenarios de posibles acontecimientos mediante los siguientes pasos:

1. Determinar los procesos donde se hará la evaluación.
2. Determinar las personas que participaran en la evaluación.
3. Determinar a los responsables de los procesos involucrados.
4. Describir el riesgo detectado.
5. Estimar la frecuencia e impacto, con relación a la materialización del riesgo.
6. Estimar y determinar la ponderación.

B) Identificar Riesgos

Para la identificación de riesgos, es importante entender el contexto externo e interno de la organización (amenazas y vulnerabilidades), de acuerdo con los procesos establecidos en el SGI.

Riesgos = (Proceso + Activos + Amenaza + Vulnerabilidad)

Identificación de activos afectados

Durante esta etapa los responsables o dueños de proceso realizan la identificación de los activos con relación a los procesos y servicios que se encuentran involucrados en el alcance del Sistema de Gestión Integral y que son

susceptibles de ser afectados por los riesgos de manera positiva y/o negativa.

1. Las personas que se encuentran involucradas en el proceso y/o servicio.
2. Los procesos o procedimientos que soportan los servicios de la organización por asegurar.
3. La infraestructura y tecnología que soporta el proceso o servicio a nivel hardware y/o software.

En esta fase es muy importante identificar si el riesgo es positivo o negativo, debido a que con base en su clasificación será el tratamiento por parte de la organización.

C) Analizar Riesgos

Se analizan las posibles amenazas y vulnerabilidades de los procesos establecidos en el alcance del SGI, evaluando conjuntamente los factores de Calidad, Seguridad, Entrega de Servicios y Continuidad.

D) Evaluar Riesgos

Los riesgos son evaluados con base a los factores de Calidad, Seguridad, Entrega de Servicios y Continuidad:

Valoración de factores 9001:2015, 20000-1:2018/ISO 22301:2019 e 27001:2013

IMPACTO DEL FACTOR	VALORES	DESCRIPCIÓN
Estrategia de Negocio	11.11	Afecta directamente los resultados esperados por la empresa
Calidad del servicio	11.11	Afecta directamente a la entrega del servicio brindado
Cliente	11.11	Afecta los requerimientos y satisfacción del cliente
Disponibilidad	11.11	Impacta la disponibilidad de los servicios de acuerdo con lo establecido contractualmente
Niveles de Servicio	11.11	Afectación en el cumplimiento de los niveles de servicio establecidos contractualmente (SLA)
Continuidad del servicio (BCP)	11.11	Interrupción de las actividades e infraestructura que soportan los servicios conforme a los tiempos objetivo.
Confidencialidad	11.11	Divulgación de información
Integridad	11.11	Alteraciones o manipulaciones en la información
Disponibilidad	11.11	Que la información no esté en tiempo cuando sea requerida

Estimación de la probabilidad para riesgos negativos
Esta actividad tiene como fin identificar la probabilidad de ocurrencia de un riesgo. Las estadísticas de los reportes relacionados con los riesgos, puede tomarse como un dato histórico de ocurrencia.

	VALORES	DESCRIPCIÓN
ALTA	9	La explotación de la amenaza puede ocurrir en cualquier momento y/o considerando que esta situación ya se ha presentado más de tres veces al año
MEDIA	6	La explotación de la amenaza puede ocurrir solo en cualquier momento bajo determinadas circunstancias y/o considerando que esta situación ya se ha presentado máximo dos veces al año
BAJA	3	La explotación de la amenaza puede ocurrir solo en circunstancias excepcionales y/o se ha presentado una vez al año
NULA	0	Nunca se ha presentado y su probabilidad es nula

Estimación de la probabilidad para riesgos positivos

Esta actividad tiene como fin identificar la probabilidad de ocurrencia de un riesgo. Las estadísticas de los reportes relacionados con los riesgos, puede tomarse como un dato histórico de ocurrencia.

	VALORES	DESCRIPCIÓN
ALTA	0	Dentro del mercado existe alta posibilidad de aprovechar la oportunidad
MEDIA	3	Existe el 50% de situaciones favorables para aprovechar la oportunidad
BAJA	6	La explotación de la oportunidad puede presentar en circunstancias excepcionales
NULA	9	Las condiciones para la explotación de la oportunidad conllevan un esfuerzo mayor para la organización

Estimación de impacto para riesgos negativos

El impacto es el nivel de afectación que tendrá el activo en el momento que se materializa el escenario de riesgo. Las consecuencias pueden ser de carácter temporal o permanente.

	VALORES	DESCRIPCIÓN
MUY ALTO	9	Pone en riesgo la situación financiera e imagen de la organización o la continuidad del negocio
ALTO	6	Impacta la operación de la organización, sin embargo, puede afectar al cliente
MEDIO	3	Desviación que puede ser tratada de manera interna a través de la mejora de procesos
BAJO	0	No existe impacto en la operación de la organización

Nivel de Riesgo = (Probabilidad X Impacto)

Estimación de impacto para riesgos positivos

El impacto es el nivel de afectación que tendrá el activo en el momento que se materializa el escenario de riesgo. Las consecuencias pueden ser de carácter temporal o permanente.

	VALORES	DESCRIPCIÓN
MUY ALTO	0	Potencializa la situación financiera e imagen de la organización, impulsando a lograr sus prioridades estratégicas y posicionamiento de la marca
ALTO	3	Incrementa la calidad y seguridad en la entrega del servicio de la organización, generando mejoras en el desempeño de los servicios
MEDIO	6	Mejoras en la operación de los procesos que contribuyen gradualmente a mejorar la eficiencia
BAJO	9	Mejoras focalizadas en las actividades operativas de la organización

Nivel de Riesgo = (Probabilidad X Impacto)

Resultado final del riesgo negativo

Riesgo Total = [(Factores de Calidad) + (Factores de Entrega de Servicios) + (Factores de Seguridad de la Información y Continuidad) + (Probabilidad X Impacto)]

VALORES	NIVEL DE RIESGO	DESCRIPCIÓN
0-45	**BAJO**	**Riesgo insignificante que no requiere acción inmediata.**
46-90	**MEDIO**	**Se debe tomar medidas para reducir el riesgo a niveles razonablemente prácticos.**
91-135	**ALTO**	**Inaceptable, deberá implementarse un tratamiento especial para su control.**
136-180	**MUY ALTO**	**Requiere acciones inmediatas con involucramiento de la Dirección General**

Resultado final del riesgo positivo

Riesgo Total = [(Factores de Calidad) + (Factores de Entrega de Servicios) + (Factores de Seguridad de la Información) + (Probabilidad X Impacto)]

VALORES	NIVEL DE RIESGO	DESCRIPCIÓN
136-180	BAJO	No requiere implementar acciones inmediatas para materializar la oportunidad
91-135	MEDIO	Requiere de implementar algunas medidas a largo plazo para materializar la oportunidad
46-90	ALTO	Requiere de implementar medidas a mediano plazo para explotar la oportunidad
0-45	MUY ALTO	Implementación de medidas inmediatas para la explotación y aprovechamiento de la oportunidad

Los riesgos positivos (oportunidades) son aquellos que su resultado va hacia tendencia cero y es identificado por la organización para establecer acciones para potencializarlos, generando beneficios.

E) Tratamiento de Riesgos

Las opciones de tratamiento del riesgo deben ser seleccionados con base en los resultados de la evaluación de la fase anterior. Los criterios para tratar los riesgos pueden ser:

- Eliminar el riesgo
- Aceptar el riesgo
- Mitigar el riesgo
- Transferir el riesgo
- Evitar el riesgo.

El plan de tratamiento de los riesgos debe tomar en cuenta el orden de prioridad para atender los mismos, es por ello por lo que deben considerar plazos de implementación.
Una vez implementados los controles se llevará a cabo la evaluación con la finalidad de identificar el riesgo residual el cual deberá ser aceptado por los dueños de los riesgos. En caso de que el nivel del riesgo no disminuya a los niveles aceptables del riesgo, la organización deberá implementar acciones que le permitan corregir e identificar de ser necesario nuevos controles los cuales le consigan los niveles aceptables.
Para el tratamiento de los riesgos negativos, se consideran aquellos cuyo resultado sea entre los valores de 91 a 180 (alto y muy alto).
En el caso de los riesgos positivos, se consideran aquellos cuyo resultado sea entre los valores de 0 a 135 (medio, alto y muy alto).

Actualizar la Declaración de Aplicabilidad de Controles (SoA)

El Líder SGI crea o actualiza la Declaración de Aplicabilidad en Tabantaj o SOA F-SGI-014 (en caso de indisponibilidad de la herramienta), tomando como base los resultados obtenidos del Análisis y Evaluación de Riesgos para justificar la selección o exclusión de controles.

5. Anexos

Los documentos que podrán utilizarse en caso de indisponibilidad de la herramienta son:

- F-SGI-011 Matriz de análisis de riesgos.
- F-SGI-012 Plan de tratamiento de riesgos.
- F-SGI-013 Carta de aceptación del riesgo.
- F-SGI-014 SoA.