RESOLUCIÓN DE GERENCIA GENERAL

N° 00137-2025-GG-OSITRAN

Lima, 5 de noviembre de 2025

VISTOS:

El Informe N° 0085-2025-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto; y el Memorando N° 0453-2025-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica; y,

CONSIDERANDO:

Que, desde el año 2005, el Ositrán tiene implementado su Sistema de Gestión de la Calidad – ISO, asimismo, desde el año 2019 implementó y certificó su Sistema de Gestión Antisoborno; además en el año 2020 el Ositrán integró en su sistema de gestión ambas normas. Como parte de la administración de dichos Sistemas de Gestión se realiza una evaluación y tratamiento de los riesgos y oportunidades asociados a su alcance;

Que, mediante Resolución N° 00037-2021-PD-OSITRAN, la Presidencia Ejecutiva aprobó la Política de Gestión Integral de Riesgos del Ositrán que establece el compromiso y los lineamientos generales sobre los cuales se efectuará la Gestión Integral de Riesgos en el Ositrán;

Que, mediante Resolución N° 0119-2021-GG-OSITRAN la Gerencia General del Ositrán aprobó el Manual de Gestión Integral de Riesgos del Ositrán, el cual establece una metodología estándar para la implementación de la Gestión del Riesgo en el Ositrán, a fin de asegurar el logro de los objetivos de la Entidad;

Que, mediante Resolución N° 020-2022-GG-OSITRAN la Gerencia General del Ositrán aprobó la modificación del Manual de Gestión Integral de Riesgos del Ositrán y su versión actualizada;

Que, mediante Resolución N° 027-2023-GG-OSITRAN la Gerencia General del Ositrán aprobó la modificación del Manual de Gestión Integral de Riesgos del Ositrán y su versión actualizada;

Que, mediante Resolución N° 081-2023-GG-OSITRAN la Gerencia General del Ositrán aprobó la modificación del Manual de Gestión Integral de Riesgos del Ositrán y su versión actualizada;

Que, mediante Resolución N° 153-2023-GG-OSITRAN la Gerencia General del Ositrán aprobó la modificación del Manual de Gestión Integral de Riesgos del Ositrán y su versión actualizada;

Que, mediante el Informe N° 0085-2025-GPP-OSITRAN de fecha 28 de octubre de 2025, la Gerencia de Planeamiento y Presupuesto, como parte de la mejora continua, sustentó la necesidad de modificar el Manual de Gestión Integral de Riesgos, razón por la cual recomendó la aprobación de la propuesta de modificación remitida;

Que, a través del Memorando N° 0453-2025-GAJ-OSITRAN de fecha 04 de noviembre de 2025, la Gerencia de Asesoría Jurídica señaló que en atención a lo establecido en los artículos 10° y 11° del Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM, la Gerencia General es la máxima autoridad administrativa del Ositrán y es responsable de aprobar normas y otros documentos e instrumentos de gestión interna, relativos a la marcha administrativa de la Institución para el cumplimiento de los órganos del Ositrán, por lo que corresponde a dicho órgano la aprobación de una norma interna a través del acto administrativo respectivo, el mismo que considera jurídicamente viable;

De conformidad con lo dispuesto en la Ley N° 26917, Ley de Supervisión de la Inversión Privada en Infraestructura de Transporte de Uso Público; el Reglamento General de Ositrán, aprobado por Decreto Supremo N° 044-2006-PCM y modificatorias; y el Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM y modificatorias;

SE RESUELVE:

Artículo 1.- Aprobar el "Manual de Gestión Integral de Riesgos del Ositrán – versión 06", que como anexo forma parte integrante de la presente resolución.

Artículo 2.- Dejar sin efecto el Manual de Gestión Integral de Riesgos del Ositrán, y sus versiones 02, 03, 04 y 05, aprobados mediante Resoluciones de Gerencia General N° 0119-2021-GG-OSITRAN, 020-2022-GG-OSITRAN, 027-2023-GG-OSITRAN, 081-2023-GG-OSITRAN, y 00152-2024-GG-OSITRAN, respectivamente.

Artículo 3.- Poner la presente Resolución en conocimiento de todas las unidades de organización del Ositrán, para difusión y aplicación.

Artículo 4.- Disponer que la Oficina de Comunicación Corporativa publique la presente Resolución en el Portal Institucional de Ositrán, ubicado en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe/ositran).

Regístrese, comuníquese y publíquese

Firmado por:
JUAN CARLOS MEJÍA CORNEJO
Gerente General
Gerencia General

Visado por:
PATRICIA REYNAGA ALVARADO
Gerente Adjunto
Gerencia General

Visado por:
JAVIER CHOCANO PORTILLO
Jefe de la Gerencia de Asesoría Jurídica
Gerencia de Asesoría Jurídica

Visado por:
ISABEL CASTILLO SIFUENTES
Jefe de la Gerencia de Planeamiento y Presupuesto (e)
Gerencia de Planeamiento y Presupuesto

NT 2025155304

MANUAL DE GESTIÓN INTEGRAL DE RIESGOS

VERSIÓN 06

Rol	Nombres y Apellidos	Cargo
Elaborado por:	Ricardo Mercado Toledo	Jefe de la Gerencia de Planeamiento y Presupuesto
Revisado por:	Ricardo Mercado Toledo	Jefe de la Gerencia de Planeamiento y Presupuesto
	Luis Miguel Torres Castillo	Jefe de Gestión de Recursos Humanos
	César Talledo León	Jefe de Tecnologías de la Información
Aprobado por:	Juan Carlos Mejía Cornejo	Gerencia General

Visado por: TALLEDO LEON Cesar Enrique FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 27/10/2025 14:15:07 -0500

Visado por: MERCADO TOLEDO Ricardo Javier FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 27/10/2025 13:11:47 -0500

Visado por: TORRES CASTILLO Luis Miguel FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 24/10/2025 16:43:09 -0500

HOJA DE CONTROL DE CAMBIOS

Versión del Manual: 06

Versión modificada	Descripción del Cambio
Versión 05	• En el numeral IV Marco Normativo, se elimina la Resolución Ministerial N° 004-2016-PCM porque ha sido derogada.
	• En el numeral IV Marco Normativo, se incorpora la Resolución Directoral N° 022-2022- INACAL/DN y Resolución de Secretaría de Gobierno y Transformación Digital N°03-2023-PCM/SGTD.
	• En el numeral 5.2 Roles y Responsabilidades se modifica el representante del SGC por representante del SIG, y se elimina representante del SGAS.
	• En el numeral 6.3.4.1 Identificación del riesgo se incorpora que en el caso de los riesgos del MI, se debe considerar los procesos operativos o misionales y los procesos de soporte que permiten a la entidad entregar sus productos.
	• En el numeral 6.3.4.3 Valoración del riesgo se incorpora que en el caso de los riesgos del MI, no se debe considerar nivel de riesgo bajo. Para los riesgos de corrupción se debe considerar un nivel alto o muy alto, y para los riesgos de inconducta funcional se debe considerar a partir del nivel medio.
	• En el numeral 6.3.5 Tratamiento del Riesgo, se incorpora precisiones para tener en cuenta sobre las medidas de control propuestas.
	• Se incorpora en el numeral 6.4 Seguimiento y revisión, se incorpora consideraciones cuando un riesgo se materializa o no.
	En el numeral 6.5 Reevaluación del riesgo, se incorpora como determinar el grado de cumplimiento de la eficacia de los riesgos.
	• En el Anexo 1 Glosario de Términos se han agregado términos vinculado con los riesgos de integridad.
	• Se modifica el Anexo 5 como Inventario de Controles Existentes y se agrega el Anexo 6 como Matriz de Comunicación del SGIR.

ÍNDICE

ACRÓNIMOS

COSO	:	Committee of Sponsoring Organizations of the Treadway
GG	:	Gerencia General
GA	:	Gerencia de Administración
GPP	:	Gerencia de Planeamiento y Presupuesto
GSF	:	Gerencia de Supervisión y Fiscalización
ISO	:	International Organization for Standardization
JGRH	:	Jefatura de Gestión de Recursos Humanos
MGPP	:	Manual de Gestión de Procesos y Procedimientos
MI	:	Modelo de Integridad
NTP	:	Norma Técnica Peruana
Ositrán	:	Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público
POI	:	Plan Operativo Institucional
SCI	:	Sistema de Control Interno
SG	:	Sistema de Gestión
SGAS	:	Sistema de Gestión Antisoborno
SGC	:	Sistema de Gestión de la Calidad
SIG	:	Sistema Integrado de Gestión
SGIR	:	Sistema de Gestión Integral de Riesgos
SGSI	:	Sistema de Gestión de Seguridad de la Información

I. OBJETIVO

Establecer una metodología estándar para la implementación de la Gestión del Riesgo en el Ositrán, a fin de coadyuvar al logro de los objetivos de la Entidad.

II. FINALIDAD

Contribuir a la consolidación de una cultura preventiva y de gestión de riesgos a través de la implementación progresiva del SGIR en el Ositrán, en el marco del proceso de Modernización de la Gestión Pública.

III. ALCANCE

Las disposiciones establecidas en el presente manual comprenden a todas las unidades de organización del Ositrán, así como a todas las personas que, bajo cualquier modalidad contractual, se encuentren vinculadas a los procesos establecidos y que constituyen un elemento de apoyo para la consecución de los objetivos de la Entidad.

IV. MARCO NORMATIVO

- Ley Nº 27658 – Ley Marco de Modernización de la Gestión del Estado y sus modificatorias.
- Ley N° 28716 – Ley de Control Interno de las Entidades del Estado y modificatorias.
- Decreto Supremo N° 092-2017-PCM, que aprueba la Política Nacional de Integridad y Lucha contra la Corrupción.
- Decreto Supremo N° 044-2018-PCM, que aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021.
- Decreto Supremo N° 123-2018-PCM, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública.
- Decreto Supremo N° 012-2015-PCM, que aprueba el Reglamento de Organización y Funciones del Ositrán.
- Resolución de Contraloría N° 146-2019-CG que aprueba la Directiva N° 006-2019-CG/INTEG “Implementación del Sistema de Control Interno en las Entidades del Estado” y sus modificatorias.
- Resolución Directoral N° 024-2017-INACAL/DN que aprueba la Norma Técnica Peruana NTP-IEC/ISO 31010:2017, Gestión del riesgo. Técnicas para la apreciación del riesgo. 1ª Edición.
- Resolución Directoral N° 014-2018-INACAL/DN que aprueba la Norma Técnica Peruana NTP-ISO 31000:2018 Gestión del riesgo. Directrices. 2a Edición y reemplaza a la NTP-ISO 31000:2011 (revisada el 2016).
- Resolución Directoral N° 001-2015-INACAL/DN que aprueba la Norma Técnica Peruana NTP-ISO 9000:2015 Sistemas de gestión de la calidad. Fundamentos y vocabulario. 6ª Edición, así como también la NTP-ISO 9001:2015 Sistemas de gestión de la calidad. Requisitos. 6ª Edición.
- Resolución Directoral N° 012-2017-INACAL/DN que aprueba la Norma Técnica Peruana NTP-ISO 37001:2017 Sistemas de gestión antisoborno. Requisitos con orientación para su uso. 1ª Edición.
- Resolución Directoral N° 022-2022- INACAL/DN, que aprueba entre otras la Norma Técnica Peruana “NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3a. Edición”.
- Resolución de Secretaría de Gobierno y Transformación Digital N°03-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, usando obligatoriamente la NTP ISO/IEC 27001 vigente.
- Resolución de Secretaría de Integridad Pública N° 002-2021-PCM/SIP que aprueba la Directiva N° 002-2021-PCM/SIP “Lineamientos para fortalecer una cultura de integridad en las entidades del sector público”.

- Resolución de Secretaría de Integridad Pública N° 001-2023-PCM/SIP que aprueba la Guía para la gestión de riesgos que afectan la Integridad Pública.

V. CONTENIDO GENERAL

5.1 OBJETIVOS DE LA GESTIÓN INTEGRAL DE RIESGOS

- Coadyuvar al logro de los objetivos de la entidad.
- Crear conciencia en las personas relacionadas contractualmente con la entidad, de la necesidad de identificar y tratar los riesgos en los procesos del Ositrán.
- Involucrar y comprometer a todos los servidores civiles del Ositrán en la búsqueda de acciones encaminadas a prevenir y gestionar los riesgos.
- Coadyuvar al logro de los objetivos de los sistemas de gestión implementados en la entidad (Calidad, Antisoborno, Seguridad de la Información), así como del Sistema de Control Interno y del Modelo de Integridad. Cumplir con la normativa vigente sobre la materia.
- Contribuir con la mejora de la Gobernanza Institucional.
- Proteger los recursos del Estado.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Contribuir a la eficacia y eficiencia operativa.
- Mejorar el aprendizaje y la flexibilidad organizacional.

5.2 ROLES Y RESPONSABILIDADES

A continuación, se presenta la organización del SGIR:

Fuente: Elaboración propia

El Órgano de Gobierno es la persona, grupo de personas u órgano que tiene la responsabilidad y autoridad final respecto de las actividades, la gobernanza y las políticas

de una organización y al cual la Alta Dirección informa y rinde cuentas. En el Ositrán se compone como sigue:

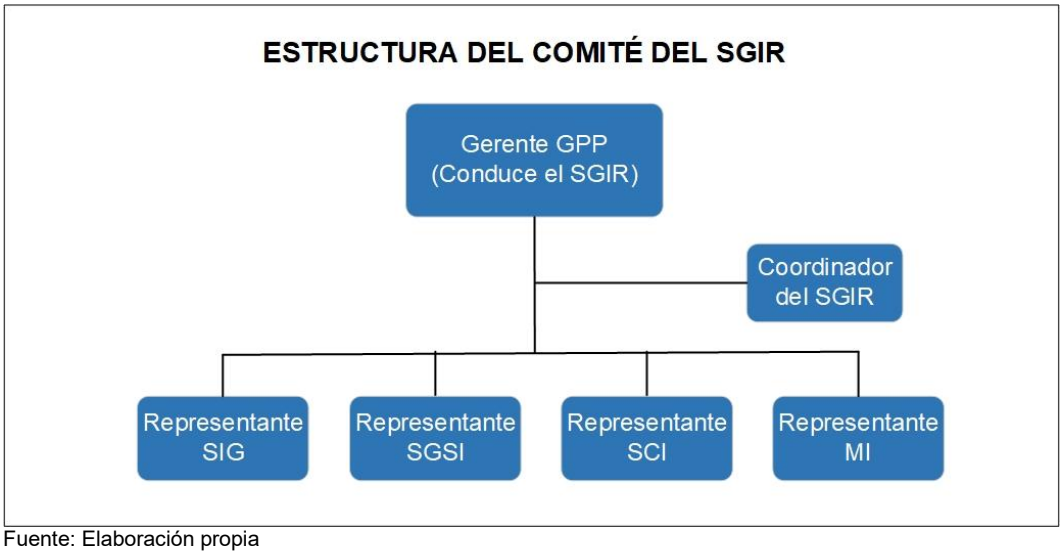
- Presidente Ejecutivo.

La Alta Dirección es la persona o grupo de personas que dirigen y controlan una organización al más alto nivel. En el Ositrán está compuesta por:

- Gerente General, quien lo preside.
- Jefa de la Gerencia de Administración.
- Gerente de Supervisión y Fiscalización.
- Jefe de la Gerencia de Planeamiento y Presupuesto.

El Comité es el grupo de personas, representantes de los sistemas de gestión y Modelo de Integridad en el alcance del SGIR. En el Ositrán está compuesto por:

- Jefe de la Gerencia de Planeamiento y Presupuesto, quien lo conduce.
- Un representante del SIG.
- Un representante del SGSI.
- Un representante del SCI.
- Un representante del MI.
- Un coordinador del SGIR, quien brinda soporte al Comité.



Fuente: Elaboración propia

La GPP tiene la responsabilidad de conducir, coordinar e implementar la gestión de riesgos en el Ositrán, en coordinación con las unidades de organización.

Los dueños de riesgos tienen la responsabilidad de identificar y evaluar periódicamente los riesgos que enfrentan sus procesos/productos. Asimismo, tienen la responsabilidad de implementar las medidas de control propuestas para tratar los riesgos, según corresponda. En adición a ello, tienen la responsabilidad de comunicar la problemática y oportunidades de mejora que hubieran identificado durante la implementación de las medidas de control a su cargo.

Es responsabilidad de los servidores civiles del Ositrán cumplir y aplicar la política de gestión integral de riesgos y sus directrices.

En el Anexo N° 02, se detallan los roles y responsabilidades del SGIR.

VI. CONTENIDO ESPECIFÍCO

6.1 CONCEPTOS BÁSICOS

Basados en la Norma ISO 31000:2018 - Guía 73 Basada 31100 y el marco integrado de Control Interno de la Contraloría General de la República, basado en el COSO.

a. Riesgo: Efecto de la incertidumbre sobre los objetivos.
Nota 1 a la entrada: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.
Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.
Nota 3 a la entrada: Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

b. Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.
Nota 1 a la entrada: Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias.
Nota 2 a la entrada: Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.
Nota 3 a la entrada: Un evento puede ser una fuente de riesgo.

c. Consecuencia: Resultado de un evento que afecta a los objetivos.
Nota 1 a la entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.
Nota 2 a la entrada: Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.
Nota 3 a la entrada: Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.

d. Probabilidad (*likelihood*): Posibilidad de que algo suceda.
Nota 1 a la entrada: En la terminología de gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo suceda esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).
Nota 2 a la entrada: El término inglés “likelihood” (probabilidad) no tiene un equivalente directo en algunos idiomas; en su lugar se utiliza con frecuencia el término probabilidad. Sin embargo, en inglés la palabra “probability” (probabilidad matemática) se interpreta frecuentemente de manera más limitada como un término matemático. Por ello, en la terminología de gestión del riesgo, “likelihood” se utiliza con la misma interpretación amplia que tiene la palabra probabilidad en otros idiomas distintos del inglés.

e. Control: Medida que mantiene y/o modifica un riesgo.
Nota 1 a la entrada: Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.
Nota 2 a la entrada: Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

f. Apetito al riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a asumir o retener.

6.2 TIPOS DE RIESGOS

En el marco de la gestión integral de riesgos, se han clasificado los siguientes tipos de riesgos que puedan presentarse, considerando el enfoque de cada sistema y Modelo de Integridad contenidos en el SGIR:

Tipos de Riesgos	Concepto
Estratégico	Asociado con la forma de administrar la institución. Se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas y el diseño y conceptualización de la institución. Puede afectar la ejecución de los procesos.
Operacional	Comprende los riesgos asociados al diseño y ejecución de los procesos, al factor humano, a las tecnologías de la información, a la comunicación y a eventos externos.
Financiero	El riesgo financiero está asociado a los riesgos de liquidez y solvencia. Está relacionado con eventos que afecten la gestión de los recursos financieros de la institución y el financiamiento de sus operaciones, siempre que no hayan sido causados directamente por factores atribuibles al riesgo operacional.
De Cumplimiento	Asociado a la capacidad de la institución para cumplir con los requisitos legales, contractuales y en general con su compromiso ante la comunidad.
De Seguridad de la Información	Que comprometan la confidencialidad, integridad o disponibilidad de los activos de información de la entidad.
De Corrupción	Posibilidad de la ocurrencia de un comportamiento, por acción u omisión, derivado del mal uso de la función o poder público, para obtener o perseguir la obtención de una ventaja o beneficio irregular, configurando un delito.
De inconducta funcional	Posibilidad de que ocurra un comportamiento, por acción u omisión, que implica el incumplimiento de funciones y que contraviene el ordenamiento jurídico administrativo y las normas internas de la entidad. De materializarse el riesgo, tendría como consecuencia la comisión de una infracción administrativa.
De Imagen	Asociados con la percepción y la confianza de las partes interesadas hacia la institución.

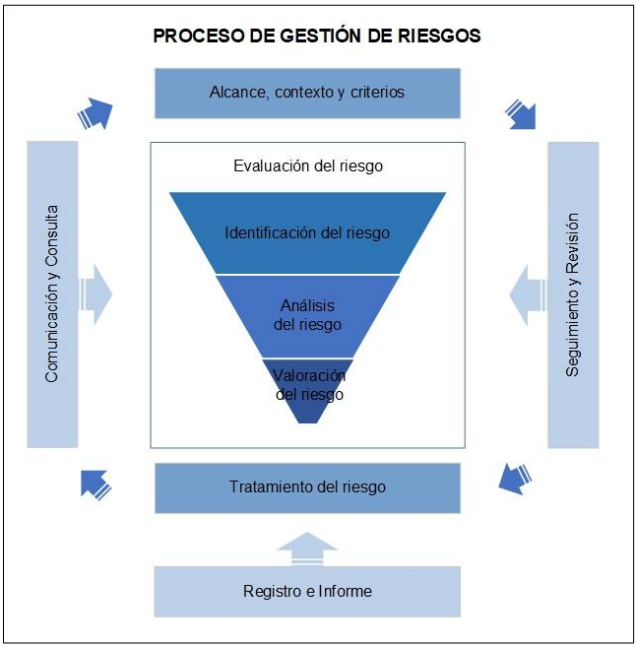
Fuente: Elaboración propia a partir de la Guía para la Administración del Riesgo[1] y de la Guía para la gestión de riesgos que afectan la integridad pública.

6.3 METODOLOGIA DE LA GESTIÓN INTEGRAL DE RIESGOS

Para la elaboración del presente manual, se ha empleado la metodología del estándar internacional ISO 31000: 2018, *Gestión del Riesgo – Directrices*, el marco integrado de Control Interno de la Contraloría General de la República, basado en el COSO y la Guía para la gestión de riesgos que afectan la integridad pública.

La óptima gestión integral de los riesgos favorece al desarrollo de la entidad y al logro de sus objetivos, contribuye a la mejora de los sistemas de gestión y a la toma de decisiones informada, por ello, es importante que se establezca el contexto del SGIR del Ositrán, la identificación, el análisis, la valoración y el tratamiento de los riesgos.

[1] Departamento Administrativo de la Función Pública – DAFP, República de Colombia.



Fuente: Elaboración propia a partir de la ISO 31000:2018

6.3.1 ESTABLECIMIENTO DEL CONTEXTO

El contexto del SGIR se debe establecer a partir de la comprensión del entorno externo e interno correspondientes al SGIR, los cuales pueden afectar la dirección estratégica del Ositrán.

Asimismo, la unidad de organización podría establecer un contexto externo e interno del proceso, en caso no este comprendido en el contexto de la dirección estratégica del Ositrán.

El contexto del SGIR se debe revisar y evaluar una vez al año, y/o cuando ocurran hechos que afecten a la organización.

En el Anexo N° 03 se describe los aspectos externos e internos que se debe considerar como mínimo para el establecimiento del contexto.

Para el caso del MI, en el Anexo N° 3 se detallan los contextos de riesgo que involucran principalmente relaciones de la entidad con actores externos y relaciones entre actores internos de la entidad.

La GPP remitirá a la GG el proyecto de contexto del SGIR debidamente visado por los titulares de las unidades de organización que son parte del alcance del SGIR.

La GG revisará el proyecto de contexto SGIR y de encontrarlo conforme, lo firmará remitiéndolo mediante memorando circular a las unidades de organización para conocimiento y a la JGRH para su publicación en la intranet institucional en coordinación con la GPP.

6.3.2 MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

Es la herramienta para la gestión integral de riesgos que cumple con los requisitos de los sistemas de gestión bajo las normas ISO, así como con la normativa aplicable en materia de control interno, resultando aplicable también para el MI que el Ositrán implemente en el marco de la lucha contra la corrupción.

Los Coordinadores del SGIR son responsables de realizar el registro de la información en la evaluación y tratamiento del riesgo en la Matriz de Gestión Integral de Riesgos.

La matriz de gestión integral de riesgos, en adelante Matriz, está representada en forma de tablas donde se detallan los criterios para la evaluación, tratamiento y reevaluación del riesgo, según el Anexo N° 04.

Los responsables de cada SG y MI gestionarán a través del SGD la aprobación de las matrices de riesgos por parte de los correspondientes dueños de los riesgos, según el alcance de cada sistema.

Los responsables de cada SG y MI remitirán la Matriz de Gestión Integral de Riesgos aprobada a la GPP, quien hará de conocimiento a los dueños de los riesgos y a la GG respecto de la versión integrada.

6.3.3 INVENTARIO Y EVALUACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de la gestión de la seguridad de la información es asegurar la preservación de la confidencialidad, integridad y disponibilidad de los activos críticos de información de la entidad. En tal sentido, resulta indispensable identificar los activos críticos del Ositrán, toda vez que los mismos constituyen el insumo principal para el proceso de evaluación y tratamiento de riesgos en materia de seguridad de la información, conforme al proceso de gestión integral de riesgos.

Para la identificación y análisis de los activos de información se debe utilizar la "Matriz de Inventario de Activos de Información".

6.3.4 EVALUACIÓN DEL RIESGO

La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo[2].

6.3.4.1 Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada[3].

En el marco de los Sistemas de Gestión aplicables a las normas ISO y MI, la unidad de organización debe considerar como entrada el análisis del contexto del Ositrán.

Para la identificación del riesgo, la unidad de organización debe considerar su MGPP identificando sus riesgos desde el proceso nivel 1 que afecten al objetivo del mismo, y evaluando la pertinencia de profundizar a otros niveles de procesos.

En el caso de los riesgos del SCI, se debe considerar lo establecido en la Directiva N° 006-2019-CG/INTEG.

[2] Numeral 6.4.1 ISO 31000: 2018
[3] Numeral 6.4.2 ISO 31000: 2018

En el caso de los riesgos del MI, se debe considerar los procesos operativos o misionales y los procesos de soporte que permiten a la entidad entregar sus productos.

En el caso de riesgos de seguridad de la información, se debe considerar los activos de información críticos de cada proceso del alcance del SGSI, identificados previamente en la "Matriz de Inventario de Activos de Información" correspondiente.

La información correspondiente a la identificación del riesgo se registra en la matriz de gestión integral de riesgos (sección de la identificación del riesgo), para lo cual se considera:

- Contexto externo e interno
- Causa que origina el riesgo
- Descripción del riesgo/oportunidad
- Efectos o consecuencias
- Tipo de riesgo
- Posible infracción administrativa o delito, en el caso del MI
- Dueño del riesgo
- Código del riesgo
- Tipo de sistema de gestión
- Posible comportamiento irregular, en el caso del MI
- Interacción o potencial agente primario, en el caso del SGAS y MI

En el Anexo N° 04 se detalla la descripción de los criterios para la identificación del riesgo.

Algunas precisiones de los riesgos:

- Al momento de identificar la debilidad considerar:
  ¿Qué debilidad podría hacer que la amenaza me genere una afectación?

- Al momento de identificar la causa considerar:
  Origen del riesgo
  ¿Qué ocasionaría dicho riesgo?

- Al momento de identificar el efecto o consecuencia considerar:
  Efecto o consecuencia debe estar asociado al objetivo del proceso/subproceso.
  ¿Qué efectos repercutirían en el subproceso de presentarse el riesgo?
  ¿Cuál es el efecto que podría ocasionar al objetivo?

- Al momento de identificar el riesgo considerar:
  La redacción del riesgo no debe confundirse con sus causas y efectos.
  ¿Qué riesgos afectan el logro del objetivo de mi subproceso?

6.3.4.2 Análisis del riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo[4].

La unidad de organización debe identificar las medidas de control existentes implementadas para el riesgo identificado.

La unidad de organización determina la eficacia de las medidas de control existentes, teniendo en cuenta los niveles y definiciones establecidos en el numeral 23 de la descripción de la Matriz, según el Anexo N° 04.

La unidad de organización debe analizar la probabilidad de ocurrencia del riesgo y el impacto de su materialización en la entidad; considerando las medidas de control existentes. Para este análisis se deberán tomar como referencia los numerales 24 y 25 de la descripción de la Matriz, según el Anexo N° 04.

A partir de la determinación de la probabilidad de ocurrencia del riesgo y su nivel de impacto, se determina el nivel de riesgo, conforme al mapa de calor del numeral 26 de la descripción de la Matriz, según el Anexo N° 04.

6.3.4.3 Valoración del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional[5].

La unidad de organización debe considerar que la línea de apetito al riesgo es hasta nivel bajo y la línea de apetito a la oportunidad es hasta nivel medio.

Para riesgos superiores a la línea de apetito, es necesario la evaluación de la amenaza versus uno o más de los siguientes factores:

a. La capacidad de recursos
b. La capacidad de control que pueda tener Ositrán frente a ella

En el caso de los riesgos del MI, no se debe considera nivel de riesgo bajo. Para los riesgos de corrupción se debe considerar un nivel alto o muy alto, y para los riesgos de inconducta funcional se debe considerar a partir del nivel medio.

En el numeral 28 de la descripción de la Matriz se detallan los tipos de respuesta para el tratamiento del riesgo, según el Anexo N° 04.

6.3.5 TRATAMIENTO DEL RIESGO

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo[6].

[4] Numeral 6.4.3 ISO 31000: 2018
[5] Numeral 6.4.4 ISO 31000: 2018
[6] Numeral 6.4.5 ISO 31000: 2018

La unidad de organización debe determinar las medidas de control propuestas para el tratamiento del riesgo, las cuales deben ser viables (sobre la base de sus propios recursos).

Las medidas de control propuestas deben ser vinculadas o incorporadas al POI, de corresponder, a fin de que se garantice su cumplimiento dentro del plazo establecido.

La información correspondiente al tratamiento del riesgo se registra en la Matriz de gestión integral de riesgos (sección de tratamiento del riesgo), para lo cual se considera:

- Medidas de control propuestas
- Medio de verificación
- Responsable de implementación
- Plazo de implementación

Una vez definido el tratamiento del riesgo, se determina el nivel de riesgo objetivo, para lo cual se estima la probabilidad de ocurrencia del riesgo y el impacto de su materialización en la entidad, que se esperan obtener luego de la implementación de las medidas de control propuestas. Ver numerales 36, 37 y 38 de la descripción de la Matriz, según el Anexo N° 04.

Algunas precisiones de las medidas de control propuestas:

- Los objetivos bien definidos proporcionan una base para evaluar la eficacia de la medida de control y medir su rendimiento:
  ¿Qué se realiza?
- Determinar las actividades o acciones específicas que deben realizarse para implementar el control de manera efectiva:
  ¿Cómo se realiza el control?
- Evaluar si se incorpora una segregación adecuada de funciones en el diseño de control.
  ¿Quién lo realiza?
- Tener en cuenta la escalabilidad y la flexibilidad del diseño del control.
  ¿Será efectivo el control a medida que la organización crezca o cambie? ¿Cuándo lo ejecuta?

6.4 SEGUIMIENTO Y REVISIÓN

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso[7].

Los responsables de los SG y MI establecen la frecuencia del seguimiento de la implementación de las medidas de control propuestas, acorde a los plazos definidos de inicio y fin, en coordinación con el responsable de la implementación. Ver numeral 39 de la descripción de la Matriz, según el Anexo N° 04.

[7] Numeral 6.6 ISO 31000: 2018

A partir del seguimiento de la implementación de las medidas de control propuestas, se determina su estado de la implementación:

Estado	Criterio
Implementado	Cuando la entidad ha cumplido con implementar la medida de control conforme la matriz de gestión integral de riesgos.
En Proceso	Cuando la entidad ha iniciado, pero aún no ha culminado con la implementación de la medida de control contenida en la matriz de gestión integral de riesgos.
Pendiente	Cuando la entidad no ha iniciado la implementación de la medida de control contenida en la matriz de gestión integral de riesgos.
No Implementado	Cuando la entidad no ha cumplido con implementar la medida de control contenida en la matriz de gestión integral de riesgos y la oportunidad para su ejecución ha culminado definitivamente.
No Aplicable	Aplicable solo a SCI. Cuando la medida de control contenida en la matriz de gestión integral de riesgos no puede ser ejecutada por factores no atribuibles a la entidad, debidamente sustentados, que imposibilitan su implementación.
Desestimado	Aplicable solo a SCI. Cuando la entidad decide no implementar la medida de control contenida en la matriz de gestión integral de riesgos, asumiendo las consecuencias de dicha decisión.

Fuente: Directiva N° 006-2019-CG/INTEG y sus modificatorias

El dueño del riesgo determina además la eficacia y mantenimiento de las medidas de control existentes anualmente, registrándose por la GPP el resultado en el numeral 40 de la descripción de la Matriz. Aplicable para el SIG, SCI y MI.

El dueño del riesgo comunica a la GPP, si el riesgo se materializó o no, como parte del seguimiento y revisión del riesgo, para lo cual se considera:

- Si se materializa el riesgo, la unidad de organización señala las medidas correctivas ejecutadas, determina la eficacia y mantenimiento de las medidas de control existentes, determinar si los controles propuestos hacen frente al riesgo y cuales no cumplieron su objetivo; de ser el caso, evalúa si es que se generó un nuevo riesgo.

- Si no se materializa el riesgo: la unidad de organización evalúa los controles existentes, indica la evidencia de la implementación de los controles propuestos y revisa el nivel del riesgo (probabilidad e impacto); de ser el caso.

Las medidas de control propuestas que son implementadas en un periodo anual se convierten en medidas de control existente para el siguiente periodo anual; registrándose por la GPP en el numeral 41 de la descripción de la Matriz. Aplicable para el SIG, SCI y MI.

A partir de la aprobación de la Matriz de Gestión Integral de Riesgos anual, los responsables de cada SG y MI, gestionan con los dueños de los riesgos, el registro de la información del Inventario de controles existentes, según el Anexo N° 5.

6.5 REEVALUACIÓN DEL RIESGO

La reevaluación del riesgo tiene como objetivo, primero determinar si los riesgos tratados mediante medidas de control propuestas alcanzaron el nivel de riesgo objetivo establecido por la unidad de organización; y, segundo, revisar la coherencia de la evaluación y tratamiento del riesgo y establecer mejoras.

Cuando las medidas de control propuestas han sido implementadas, la unidad de organización, en coordinación con la GPP, deben reevaluar anualmente los riesgos, aplicando para ello, los numerales 42, 43 y 44 de la descripción de la Matriz, según el Anexo N° 04.

Una vez definido el nivel del riesgo reevaluado, la unidad de organización determina el nivel de eficacia de los controles propuestos comparando el nivel de riesgo reevaluado con el nivel de riesgo objetivo:

- Se registra "Sí", cuando el nivel de riesgo reevaluado es menor o igual al nivel de riesgo objetivo y si se obtiene o disminuye la probabilidad objetivo.

- Se registra "No" cuando el nivel de riesgo reevaluado es mayor que el nivel de riesgo objetivo o se incrementa la probabilidad objetivo, ver numeral 46 de la descripción de la Matriz, según el Anexo N° 04.

Cuando la unidad de organización determine que las medidas de control propuestas no fueron eficaces, es decir que los riesgos identificados no alcanzaron el nivel de riesgo objetivo, se deben determinar nuevas medidas de control propuestas. En caso el riesgo identificado no logre mitigarse puede realizarse hasta máximo una segunda reevaluación. Pasada dos reevaluaciones sin mitigar el riesgo, el Comité de SGIR reporta a la Alta Dirección del SGIR, a fin de evaluar el tipo de respuesta que corresponda luego del análisis y evaluación.

Culminada la reevaluación, los responsables de cada SG y MI determinan el grado de cumplimiento de la eficacia de los riesgos, para lo cual se considera:

$$\frac{\text{Total de riesgos con eficacia “Si” x 100\%}}{\text{Total de riesgos identificados}}$$

6.6 COMUNICACIÓN Y CONSULTA

El propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones[8].

La GPP determina la planificación de actividades para asegurar la eficacia de la comunicación utilizando la Matriz de comunicaciones del SGIR, según el Anexo N° 06.

La matriz de comunicación comprende: Qué se comunica, cuándo se comunica, a quién se comunica, cómo se comunica, quién comunica, idiomas y toma de conciencia.

Las comunicaciones deben ser veraces, pertinentes, exactas, entendibles y de integridad a fin de evitar percepciones equivocadas del riesgo, de tal manera que permita tomar decisiones acertadas y eficaces.

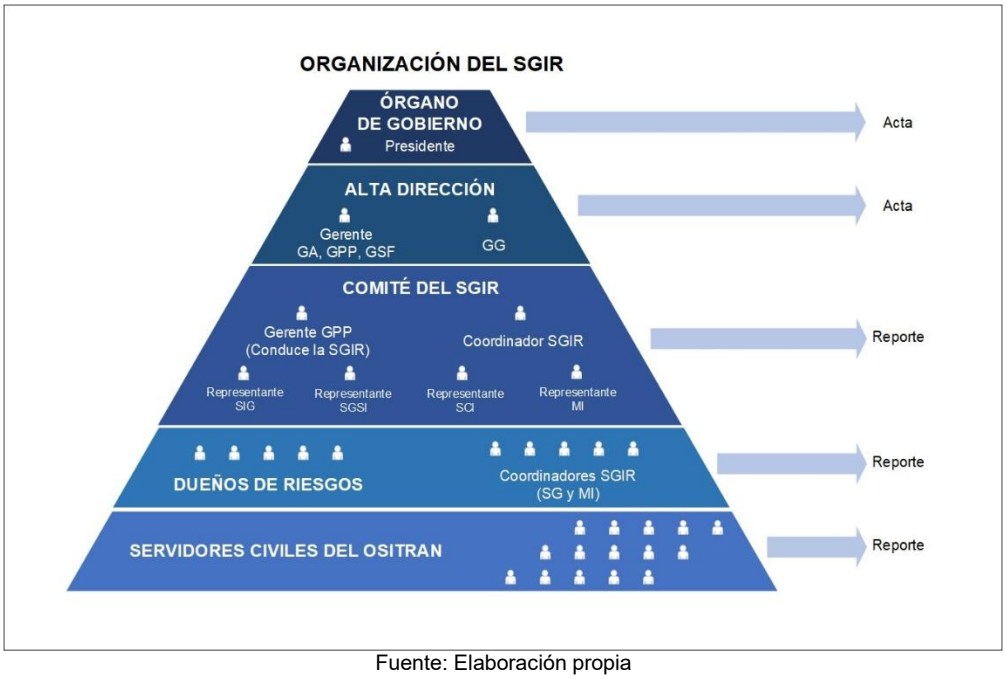
[8] Numeral 6.2 ISO 31000: 2018

La GPP recabará información sobre las mejoras del SGIR con los dueños de los riesgos, los responsables de la implementación de las medidas de control propuestas y los coordinadores del SGIR de cada sistema de gestión y Modelo de Integridad. En base a dicha información, la GPP podrá plantear medidas para la mejora continua del SGIR.

6.7 REGISTRO E INFORMES

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados[9].

A continuación, se muestra la estructura documentaria según los roles y responsabilidades del SGIR:



Fuente: Elaboración propia

Los responsables de la implementación de las medidas de control propuestas informan al coordinador del SGIR sobre los avances de la ejecución de las medidas de control propuestas y el mantenimiento de las medidas de control existentes.

A partir de ello, los coordinadores del SGIR de cada sistema de gestión y Modelo de Integridad consolidan la información y elaboran un reporte anual para ser remitido al Comité del SGIR.

El coordinador del Comité del SGIR revisa los reportes sobre los avances de la ejecución de las medidas de control propuestas, el mantenimiento de las medidas de control existentes y elabora el reporte ejecutivo sobre el SGIR, el cual es aprobado por el Comité del SGIR y dirigido a la Alta Dirección.

La Alta Dirección del SGIR y el Órgano de Gobierno del SGIR emiten mediante Actas, la revisión de la información, análisis de los datos, decisiones y acciones de mejora del SGIR, de manera anual.

[9] Numeral 6.7 ISO 31000: 2018

VII. ANEXOS

Anexo N° 01: GLOSARIO DE TERMINOS

Anexo N° 02: ROLES Y RESPONSABLES DEL SGIR

Anexo N° 03: ESTABLECIMIENTO DEL CONTEXTO EXTERNO E INTERNO

Anexo N° 04: MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

Anexo N° 05: INVENTARIO DE CONTROLES EXISTENTES

Anexo N° 06: MATRIZ DE COMUNICACIONES DEL SGIR

ANEXO N° 01

GLOSARIO DE TERMINOS

- Activo: Cualquier recurso que tiene valor para la organización y que por lo tanto requiere protección.
- Activo de Información: Activos asociados al almacenamiento o tratamiento de la información.
- Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados
- Eficacia: Grado en el que se realizan las actividades planificadas y se logran los resultados planificados
- Dueños de Riesgos: Unidad de organización que rinde cuentas del desempeño de sus riesgos.
- Medida de control existente: Medida que se emplea actualmente para controlar o reducir el riesgo o detectar la oportunidad, como políticas, procedimientos, técnicas u otros mecanismos.
- Medida de control propuesta: Medida que permite reducir de manera eficaz el riesgo o aprovechar la oportunidad, como políticas, procedimientos, técnicas u otros mecanismos.
- Medio de verificación: Documentos u otros medios que permiten comprobar la implementación de las medidas de control propuestas.
- Modelo de Integridad: Es el conjunto de orientaciones organizadas de manera sistémica en componentes, para fortalecer la capacidad de prevención y de respuesta de las entidades públicas frente a la corrupción y diversas prácticas antiéticas. Supone el desarrollo de un trabajo articulado y colaborativo entre las unidades de organización para implementar el enfoque de integridad pública, incluyendo el cumplimiento de normas, la adopción de buenas prácticas de integridad; así como la implementación de directrices, lineamientos, guías, herramientas y mecanismos necesarios para su implementación.
- Parte Interesada: Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- Responsables de implementación: Unidad de organización que implementa las medidas de control propuestas.
- Riesgos que afectan la integridad pública: es la posibilidad de que un determinado comportamiento transgreda, por acción u omisión, el respeto de los principios, deberes y normas relacionadas al ejercicio de la función pública, así como los valores de la organización, y configure una práctica contraria a la ética.
- Riesgo de corrupción: Posibilidad de que ocurra un comportamiento, por acción u omisión, derivado del mal uso de la función o poder público, para obtener o perseguir la obtención de una ventaja o beneficio irregular, lo cual configura un delito. En caso de materializarse el riesgo, tendría como consecuencia la comisión de un delito contra la administración pública, sin perjuicio de posibles implicancias en el ámbito civil y/o administrativo.
- Riesgo de inconducta funcional: Posibilidad de que ocurra un comportamiento, por acción u omisión, que implica el incumplimiento de funciones y que contraviene el ordenamiento jurídico administrativo y las normas internas de la entidad. En caso de materializarse el riesgo, tendría como consecuencia la comisión de una infracción administrativa, sin perjuicio de posibles implicancias en el ámbito civil y/o penal.

- Procesos misionales: Procesos operativos o misionales, desarrollados por los órganos de línea, que permiten la producción y entrega de los productos (bienes, servicios y/o regulaciones) que brinda la entidad a la población.

- Procesos de soporte: Procesos de soporte, desarrollados por los órganos de apoyo y de asesoramiento, que proporcionan los recursos para la consecución de los productos que brinda la entidad a la población, tales como: gestión de recursos humanos, abastecimiento, inversiones, presupuesto, tesorería, etc.

- Producto: Bien o servicio que proporcionan las entidades/dependencias del Estado a una población beneficiaria con el objeto de satisfacer sus necesidades.

- Sistema de Control Interno: Es el conjunto de acciones, actividades, planes, políticas, normas, registros, organización, procedimientos y métodos, incluyendo la actitud de las autoridades y del personal, organizado e instituido en cada entidad del Estado, para la consecución de sus objetivos.

- Viable: Dicho de un asunto que, por circunstancias tiene probabilidades de poderse llevar a cabo.

- Además, deberán considerarse otras definiciones y términos considerados en la Guía para la gestión de riesgos que afectan la integridad pública.

ANEXO N° 02

ROLES Y RESPONSABLES DEL SGIR

Estructura	Órgano de Gobierno del SGIR	Alta Dirección del SGIR	Comité del SGIR	Gerencia de Planeamiento y Presupuesto (Conduce el GIR)	Coordinador SGIR (GPP)	Coordinador SGIR (Del alcance proceso/producto del SG)	Dueños de Riesgos	Servidores Civiles del Ositrán
Rol	**Rol**: Entiende, cumple y aplica las directrices del SGIR, en lo relacionado con su rol en la organización.	**Rol**: Entiende, cumple y aplica las directrices del SGIR, en lo relacionado con su rol en la organización.	**Rol**: Verifica el funcionamiento del SGIR.	**Rol**: Conduce, coordina e implementa la gestión del riesgo en el OSITRÁN, en coordinación con las unidades de organización.	**Rol**: Monitorea el cumplimiento de las directrices del SGIR.	**Rol**: Gestiona y monitorea el cumplimiento de las directrices de gestión del riesgo de los procesos/productos en el alcance de los SG.	**Rol**: Rinde cuentas del desempeño de sus riesgos.	**Rol**: Cumple y aplica la política de gestión integral de riesgos y las directrices del SGIR.
Responsabilidades	**Responsabilidades**: a. Aprobar la política del SGIR. b. Asegurar que la política y las estrategias de la entidad estén alineadas. c. Disponer los recursos para el funcionamiento eficaz del SGIR. d. Recibir, revisar y supervisar a intervalos planificados la información sobre el contenido y el funcionamiento del SGIR, información que le proporciona la Alta Dirección sobre la implementación y eficacia del SGIR.	**Responsabilidades**: a. Asegurar que el SGIR, incluyendo la política y los objetivos, se establezcan, implementen, mantengan y revisen, de modo que aborden adecuadamente los riesgos de los sistemas de gestión de la organización y que estén alineados con los objetivos de la Entidad. b. Asegurar que las directrices del SGIR se integren en los procesos de la organización. c. Desplegar los recursos suficientes para el funcionamiento eficaz del SGIR. d. Comunicar interna y externamente la política del SGIR. e. Promover una cultura de la gestión del riesgo dentro de la organización, a través la sensibilización y toma de conciencia. f. Promover la mejora continua. g. Revisar el SGIR a intervalos planificados para asegurarse de su idoneidad, adecuación y eficacia continuas, reportando al órgano de gobierno sobre el contenido, funcionamiento y resultados del SGIR. h. Asegurar que las funciones, responsabilidades y autoridades para los roles pertinentes sean asignadas y comunicadas, a todos los niveles de la organización.	**Responsabilidades**: a. Revisar la Política, los objetivos del SGIR y su planificación, proponiendo la actualización cuando corresponda. b. Asegurar que la Política del SGIR se encuentre implementada. c. Promover la implementación de la gestión del riesgo en los procesos del alcance de los Sistema de Gestión que forman parte del SGIR. d. Promover y gestionar la implementación, mantenimiento y mejora del SGIR. e. Verificar periódicamente el desempeño y eficacia del SGIR. f. Diseñar y planificar las actividades de sensibilización del SGIR.	**Responsabilidad**: a. Velar por el cumplimiento de las responsabilidades del Comité del SGIR. b. Asesorar en la implementación, evaluación y mejora de la gestión del riesgo en los SG y MI. c. Recabar información a fin de retroalimentar el SGIR sobre la base de buenas prácticas, lecciones aprendidas e información relevante para la mejora continua.	**Responsabilidad**: a. Coordinar e implementar las actividades destinadas a la evaluación de riesgos de gestión, en el marco de las disposiciones sobre la materia. b. Consolidar los reportes recabados en el marco del SGIR. c. Proponer acciones para la mejora del desempeño y eficacia del SGIR.	**Responsabilidad**: a. Consolidar y mantener la información relacionada a los riesgos de los procesos/productos en el alcance de los SG.	**Responsabilidad**: a. Identificar y evaluar periódicamente los riesgos que enfrenta en sus procesos/productos e implementar las medidas de control para mitigar los riesgos.	**Responsabilidad**: a. Cumplir y aplicar la política de gestión integral de riesgos y las disposiciones del SGIR.

Fuente: Elaboración propia

ANEXO N° 03

ESTABLECIMIENTO DEL CONTEXTO EXTERNO E INTERNO

Análisis del contexto externo

Comprende realizar un análisis considerando los siguientes aspectos:

Aspectos Externos	Descripción
Políticas de Gobierno	Legislación, políticas públicas, regulación.
Cambios en la legislación	Modificaciones normativas, dispositivos.
Evolución tecnológica	Interrupciones, tecnología emergente, transformación digital, big data.
Contexto económico	Recaudación, normatividad presupuestal, sentencias judiciales.
Contexto Social	Corrupción
Interacción con las partes interesadas externas sobre los servicios prestados	Concesionarios, proveedores, empresas supervisoras.
Lugares donde se desarrolla el servicio	Localización de las concesiones.
Relación con funcionarios públicos	Interacción con funcionarios de entidades vinculadas con Ositrán.

Fuente: Elaboración propia

Análisis del contexto interno

Comprende realizar un análisis considerando los siguientes aspectos:

Aspectos Internos	Descripción
Cultura Organizacional	La cultura organizacional es la esencia de cada entidad pública y está presente en todas las acciones que realizan sus servidores[10].
Competencia del personal	Educación, formación y experiencia.
Conocimiento Organizativo y Gestión del Conocimiento	Conocimiento de la organización y del Sistema de Gestión y Modelo de Integridad; así como la Gestión del Conocimiento.
Recursos Financieros	Presupuesto
Valores institucionales	Son el eje fundamental de la cultura organizacional, pues determinan la manera de actuar de todos sus miembros[11].
Estructura Organizacional	Niveles para la toma de decisiones.
Comunicación Interna	Define la forma de intercambio de información en la entidad y es elaborado de acuerdo a la

[10] Numeral 2.1 de la Guía para la Gestión del Proceso de Cultura y Clima Organizacional del Sistema Administrativo de Gestión de Recursos Humanos, aprobada con Resolución de Presidencia Ejecutiva N° 150-2017-SERVIR-PE.
[11] Fase I: Planificación de la Guía para la Gestión del Proceso de Cultura y Clima Organizacional del Sistema Administrativo de Gestión de Recursos Humanos, aprobada con Resolución de Presidencia Ejecutiva N° 150-2017-SERVIR-PE.

Aspectos Internos	Descripción
	Guía para el proceso de Comunicación Interna[12].
Tecnologías Utilizadas:	Aplicativos, sistemas, softwares, que utiliza la entidad.
Enfoque al cliente:	Capacidad de los procesos del Ositrán para interactuar y asegurar el cumplimiento de los requisitos asociados con los servicios que brinda.
Eficacia de las medidas de control existentes	Capacidad que tiene el control implementado para lograr el objetivo esperado.
Desempeño de procesos	Capacidad de los procesos para contribuir al logro de sus objetivos.
Liderazgo de la Alta Dirección	Compromiso que evidencia la Alta Dirección con la implementación de la Gestión Integral de Riesgos en los procesos del Ositrán.
Alineación con los Objetivos Estratégicos de la Institución	Es la capacidad que tiene el SGIR para prevenir y anticiparse a escenarios que puedan afectar el logro de los objetivos de la Entidad.

Fuente: Elaboración propia

Para el caso del MI, es posible identificar circunstancias en las cuales un servidor público sea más propenso a prácticas que afecten la integridad pública. A continuación, se detallan los contextos de riesgo que involucran principalmente relaciones de la entidad con actores externos y relaciones entre actores internos de la entidad:

Contextos	Concepto
Compra de bienes	Referido a la adquisición de objetos que requiere una entidad para el desarrollo de sus actividades y cumplimiento de sus fines.
Contratación de obras	Referido a la contratación para la construcción, reconstrucción, remodelación, mejoramiento, demolición, renovación, ampliación o habilitación de bienes inmuebles, tales como edificaciones, estructuras, excavaciones, perforaciones, carreteras, puentes, entre otros.
Contratación de servicios	Referido a la contratación de servicios o consultorías requeridos por una entidad para el desarrollo de sus actividades y el cumplimiento de sus funciones y fines.
Contratación y gestión de personal	Referido al ingreso, la permanencia o evaluación de servidores públicos (incluye verificación de la idoneidad, procedimientos administrativos-disciplinarios, entre otros).
Prestación directa de servicios a los usuarios	Referido a la entrega de servicios con interacción directa entre los usuarios y el servidor público. Puede referirse a servicios de salud, educación, limpieza, serenazgo, entre otros.
Fiscalización, supervisión o monitoreo	Referido a las funciones de fiscalización para verificar el cumplimiento de condiciones de operación en el ámbito laboral, de transporte, ambiental, etc. Asimismo, se incluyen tareas de supervisión que realiza una entidad pública sobre una actividad, para comprobar si el personal cumple con sus obligaciones y establecer acciones correctivas de detectarse algún incumplimiento.
Elaboración o aprobación de normas	Referido al desarrollo y emisión de leyes, resoluciones, ordenanzas, decretos, directivas, etc.

[12] Guía para la Gestión del Proceso de Comunicación Interna del Sistema Administrativo de Gestión de Recursos Humanos, aprobada con Resolución de Presidencia Ejecutiva N° 151-2017-SERVIR-PE.

Contextos	Concepto
Emisión de autorizaciones	Referido a los actos administrativos de una entidad que tiene por finalidad autorizar el funcionamiento, operación o realización de diversas actividades.
Gestión de dinero entregado a servidores de la entidad	Referido al uso y rendición de dinero entregado a servidores para el cumplimiento de tareas o funciones determinadas.
Pago a proveedores	Referido al proceso de aprobación y pago a proveedores de la entidad.
Recaudación directa de ingresos	Referida a los ingresos directamente recaudados, tributarios (impuestos, contribuciones, tasas) y no tributarios (por los servicios que prestan a sus usuarios), por parte de la entidad.
Servicios administrativos	Referido a los productos que genera una entidad para otras entidades públicas (usuarias), como un medio o soporte para la optimización de su gestión interna o la prestación eficiente y de calidad de los bienes y servicios que prestan.
Otro contexto	No previsto en los contextos descritos anteriormente.

Fuente: Guía para la gestión de riesgos que afectan la Integridad Pública.

ANEXO N° 04

MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

ÁREA / PROCESO / SUB PROCESO / OBJETIVO / ACTIVO						EVALUACIÓN																												TRATAMIENTO										SEGUIMIENTO			REEVALUACIÓN DEL RIESGO (Después de implementada la medida de control)				
						IDENTIFICACIÓN																					ANÁLISIS						VALORACIÓN																		
							CONTEXTO EXTERNO	CONTEXTO INTERNO									16. TIPO SISTEMA DE GESTIÓN						INTERACCIÓN																PLAZO DE IMPLEMENTACIÓN		DETERMINACIÓN DEL NIVEL DE RIESGO OBJETIVO										
1. UNIDAD DE ORGANIZACIÓN	2. PROCESO	3. SUB PROCESO	4. OBJETIVO	5. ACTIVO	6. PRODUCTO PRIORIZADO	7. CONTEXTOS (Aplicable solo al MI)	7.1 OPORTUNIDAD / AMENAZA	7.2 FORTALEZA / DEBILIDAD / VULNERABILIDAD	8. CAUSA	9. RIESGO/ OPORTUNIDAD IDENTIFICADO	10. EFECTO O CONSECUENCIA	11. RIESGO U OPORTUNIDAD	12. TIPO DE RIESGO	13. POSIBLE INFRACCIÓN ADM O DELITO	14. DUEÑO DEL RIESGO	15. CODIGO	SGC	SGAS	SGSI	SCI	MI	17. POSIBLE COMPORTAMIENTO IRREGULAR (Aplicable solo al MI)	18. POTENCIAL AGENTE PRIMARIO	19. PARTES INTERESADAS RELACIONADAS POTENCIALES AGENTES EXTERNOS (Aplicable solo al SGAS y MI)	20. PUESTOS INVOLUCRADOS O POTENCIALES AGENTES INTERNOS (Aplicable solo al SGAS y MI)	21. PREGUNTAS DE VALIDACIÓN (Aplicable solo al MI)	22. MEDIDAS DE CONTROL EXISTENTES	23. EFICACIA DE MEDIDAS DE CONTROL EXISTENTES	24. PROBABILIDAD (P)	25. IMPACTO (I)	26. NIVEL DE RIESGO (NR)	27. PRIORIZACIÓN (Aplicable solo al SGSI)	28. TIPO DE RESPUESTA	29. MEDIDAS DE PREVENCIÓN O MITIGACIÓN (Aplicable solo al MI)	30. MEDIDAS DE CONTROL PROPUESTOS	31. CONTROLES ASOCIADOS A LA ISO 27001	32. MEDIO DE VERIFICACIÓN	33. RESPONSABLE DE IMPLEMENTACIÓN	34. FECHA DE INICIO	35. FECHA DE TÉRMINO	36. PROBABILIDAD (P)	37. IMPACTO (I)	38. NIVEL DEL RIESGO (NR)	39. FRECUENCIA DE SEGUIMIENTO	40. ESTADO DE LA IMPLEMENTACIÓN	41. OBSERVACIÓN/ COMENTARIO	42.PROBABILIDAD (P)	43. IMPACTO (I)	44. NIVEL DEL RIESGO (NR)	45. FECHA DE EVALUACIÓN DE EFICACIA	46. EFICACIA

Fuente: Elaboración propia

DESCRIPCIÓN DE LA MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

<table>
<tr><th>NUMERALES
ÁREA/PROCESO/SUB PROCESO</th><th>DESCRIPCIÓN</th></tr>
<tr><td>1. ÓRGANO/UNIDAD ORGÁNICA/OFICINA/ÁREA</td><td>Indicar el órgano, unidad orgánica, oficina o área al que pertenece el proceso.</td></tr>
<tr><td>2. PROCESO</td><td>Registrar el proceso que puede verse afectado.</td></tr>
<tr><td>3. SUBPROCESO</td><td>Registrar el subproceso que puede verse afectado, tomando en cuenta el de menor nivel.</td></tr>
<tr><td>4. OBJETIVO</td><td>Registrar la razón de ser del subproceso/proceso, tomando en cuenta el de menor nivel.</td></tr>
<tr><td>5. ACTIVO</td><td>Registrar el nombre del activo crítico sobre la base de la matriz de inventarios activos de información. Aplicable solo al SGSI.</td></tr>
<tr><td>6. PRODUCTO PRIORIZADO</td><td>Registrar el producto priorizado que puede verse afectado, en caso corresponda. Aplicable solo al SCI.</td></tr>
<tr><td colspan="2">EVALUACIÓN DEL RIESGOS</td></tr>
<tr><td colspan="2">IDENTIFICACIÓN DEL RIESGO</td></tr>
<tr><td>7. CONTEXTOS (Aplicable solo al MI)</td><td>Es posible identificar circunstancias en las cuales un servidor público sea más propenso a prácticas que afecten la integridad pública. En el Anexo 2 se describen los contextos de riesgo que involucran principalmente relaciones de la entidad con actores externos y relaciones entre actores internos de la entidad.</td></tr>
<tr><td>7.1 OPORTUNIDAD/AMENAZA</td><td>Registrar la Oportunidad o Amenaza que podría afectar el logro de los objetivos, asociada con el numeral 4, o a la seguridad del activo de información identificado en el numeral 5, en el caso de riesgos del SGSI.</td></tr>
<tr><td>7.2 FORTALEZA/DEBILIDAD/ VULNERABILIDAD</td><td>Registrar Fortaleza o Debilidad o vulnerabilidad, asociada con el numeral 7.1.</td></tr>
<tr><td>8. CAUSA</td><td>Registrar la causa que origina el riesgo u oportunidad. No aplicable a SGSI, toda vez que la causa ya está expresada en términos de la vulnerabilidad y la amenaza.
Para el caso del MI, consignar el tipo de causa según sea el caso:
• Las causas personales (CP): referidas a los potenciales agentes de riesgo al interior de la institución.
• Las causas organizacionales (CO): referidas a la entidad y su funcionamiento, tomando en cuenta la estrategia institucional y la estructura definida, así como las prácticas informales que la sostienen.

<table>
<tr><th>Causas</th><th>Concepto</th></tr>
<tr><td>Predisposición por relación personal (CP)</td><td>Relación o vinculación del servidor con una persona o grupo de personas que podría llevarlo a actuar sin imparcialidad en los asuntos a su cargo o favorecer determinados intereses particulares. Por ello, el servidor podría tender a favorecer a familiares, socios, colegas, amistades o grupo de personas conocidas, incluso sin una solicitud expresa, para asentar su vínculo o relación.</td></tr>
<tr><td>Falta o deterioro de carácter ético (CP)</td><td>Deterioro gradual de los estándares de integridad personal del servidor que lo podría predisponer a pasar por alto cualquier freno o restricción que le impida la comisión de una práctica contraria a la</td></tr>
</table>
</td></tr>
</table>

NUMERALES	DESCRIPCIÓN	
		ética, especialmente en contextos organizacionales con una cultura de integridad deteriorada, poco afianzada o en proceso de fortalecimiento.
	Percepción de impunidad (CP)	Situación que podría llevar a un servidor, consciente de las consecuencias existentes frente a una trasgresión, a incumplir deliberadamente un deber o no observar una prohibición porque percibe que su actuación podría no ser detectada o tendría baja probabilidad de serlo. En ese sentido, percibe que el eventual costo de su acción (posible sanción) será menor que el potencial beneficio.
	Desconocimiento (CP)	Situación que podría llevar al servidor a una transgresión por desconocimiento de sus deberes, obligaciones y/o de las consecuencias derivadas de su incumplimiento al interpretar que una decisión podría ser aceptable, en un determinado contexto.
	Presión jerárquica o de pares (CO)	Situación derivada de la presión de un superior jerárquico o de pares sobre el servidor para alcanzar un fin determinado (por interés particular o institucional), lo que podría considerar o no posibles consecuencias, afectando la observancia de valores, principios y normas.
	Procesos ineficientes (CO)	Situación derivada de procesos mal diseñados, regulación deficiente o insuficiente; o ambigüedad en las instrucciones o existencia de indicaciones contrapuestas que podría llevar al servidor a una práctica contraria a la integridad pública.
	Alta discrecionalidad (CO)	Situación derivada del poder otorgado al servidor público para tomar ciertas decisiones sin que sea requerido a solicitar autorización o a informar sobre sus decisiones y a justificarlas.
	Práctica normalizada (CO)	Situación derivada de los usos y costumbres de la organización o su entorno (en relación con sus públicos de interés) que podrían dar paso a prácticas antiéticas o corruptas.
9. RIESGO/OPORTUNIDAD IDENTIFICADO	Describir las características generales o las formas en que se observa o manifiesta el riesgo u oportunidad. Para el caso del MI, el riesgo se redacta de la siguiente manera: *Agente(s) podría(n) [posible comportamiento irregular] en contexto de riesgo*.	

<table>
<tr><th>NUMERALES</th><th>DESCRIPCIÓN</th></tr>
<tr><td>10. EFECTO O CONSECUENCIA</td><td>Describir el impacto que podría generar el riesgo u oportunidad con respecto a los objetivos o a la seguridad del activo de información.
Para el caso del MI, consignar el tipo de efecto según sea el caso:

<table>
<tr><th>Efectos</th><th>Concepto</th></tr>
<tr><td>Afectación de derechos</td><td>Se afecta (restringe o impide) el acceso a derechos (fundamentales, sociales, económicos o políticos) de los públicos de interés (ciudadanía, trabajadores de la entidad, usuarios o administrados, representantes del ámbito privado, entidades públicas clave, entre otros).</td></tr>
<tr><td>Afectación de servicios</td><td>Se afecta el acceso o la continuidad de los servicios que se prestan a los usuarios o población atendida por la entidad.</td></tr>
<tr><td>Pérdida o desvío de bienes o recursos de la entidad</td><td>Los bienes y/o recursos (del tesoro, los contribuyentes u otra fuente) se pierden o emplean para un uso no permitido.</td></tr>
<tr><td>Afectación del patrimonio o recursos de los usuarios</td><td>El requerimiento o aceptación de un beneficio indebido por parte de los funcionarios o servidores afecta el patrimonio o recursos de los usuarios o administrados.</td></tr>
<tr><td>Afectación a la continuidad de la actual gestión (titular)</td><td>La continuidad de la gestión de la entidad podría interrumpirse o finalizar antes de lo previsto debido a la gravedad del hecho.</td></tr>
</table>
</td></tr>
<tr><td>11. RIESGO U OPORTUNIDAD</td><td>Registrar si se considera un riesgo (negativo) o una oportunidad (positivo).</td></tr>
<tr><td>12. TIPOS DE RIESGOS</td><td>Utilizar los tipos de riesgos según sea el caso.</td></tr>
</table>

NUMERALES	DESCRIPCIÓN

Tipos de Riesgos	Concepto
Estratégico	Asociado con la forma de administrar la institución. Se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas y el diseño y conceptualización de la institución. Puede afectar la ejecución de los procesos.
Operacional	Comprende los riesgos asociados al diseño y ejecución de los procesos, al factor humano, a la tecnología de información, a la comunicación y a eventos externos. No incluye riesgo estratégico, ni de reputación.
Financiero	El riesgo financiero está asociado a los riesgos de liquidez y solvencia. Está relacionado con eventos que afecten la gestión de los recursos financieros de la institución y el financiamiento de sus operaciones, siempre que no hayan sido causados directamente por factores atribuibles al riesgo operacional.
De Cumplimiento	Asociado a la capacidad de la institución para cumplir con los requisitos legales, contractuales y en general con su compromiso ante la comunidad.
De Seguridad de la Información	Que comprometan la Confidencialidad, Integridad o Disponibilidad de los activos de información de la entidad.
De Corrupción	Posibilidad de que ocurra un comportamiento, por acción u omisión, derivado del mal uso de la función o poder público, para obtener o perseguir la obtención de una ventaja o beneficio irregular, lo cual configura un delito
De inconducta funcional	Posibilidad de que ocurra un comportamiento, por acción u omisión, que implica el incumplimiento de funciones y que contraviene el ordenamiento jurídico administrativo y las normas internas de la entidad
De Imagen	Asociados con la percepción y la confianza de las partes interesadas hacia la institución.

13. POSIBLE INFRACCIÓN ADMINISTRATIVA O DELITO (Aplicable solo al MI)	Registrar las inconductas funcionales que constituyen infracciones administrativas pasibles de sanción o los delitos contra la administración pública que involucran a servidores públicos de manera unilateral, en acuerdo con otro(s) servidor(es) público(s) o en complicidad con particulares (individuos o empresas). Estos delitos están tipificados en el Capítulo II del Título XVIII del Código Penal.
14. DUEÑO DEL RIESGO	Registrar la unidad de organización que es responsable de la gestión del riesgo y de rendir cuentas del desempeño del mismo.
15. CÓDIGO	Registrar OP si es oportunidad y RI si es riesgos, seguido de las siglas del sistema de gestión que corresponde, así como del código del proceso y la numeración correlativa en dos dígitos.
16. TIPO DE SISTEMA	Registrar con SGC (De Calidad) o SGAS (Antisoborno) o SGC / SGAS de ser ambos sistemas o SGSI (Seguridad de la Información) o SCI (Control Interno) o MI (Modelo de Integridad).

<table>
<tr><th>NUMERALES</th><th>DESCRIPCIÓN</th></tr>
<tr><td>17. POSIBLE COMPORTAMIENTO IRREGULAR (Aplicable solo al MI)</td><td>Los comportamientos comúnmente asociados a prácticas que afectan la integridad pública son:
<table>
<tr><th>Posible comportamiento irregular</th><th>Concepto</th></tr>
<tr><td>Apropiación o uso indebido de recursos, bienes o información del Estado</td><td>Cuando el servidor se adueña o utiliza de manera indebida dinero, recursos (incluyendo el tiempo asignado a la función pública), bienes o información del Estado.</td></tr>
<tr><td>Favorecimiento indebido</td><td>Cuando el servidor utiliza su cargo para favorecer irregularmente a alguna persona por un interés particular o interés ajeno al cumplimiento de sus funciones.</td></tr>
<tr><td>Acceso a ventajas indebidas (incluye soborno)</td><td>Cuando el servidor propicio, solicito o acepto alguna ventaja o beneficio indebido (dinero, regalos, donaciones a título personal, bienes, incentivos, cortesías o favores).</td></tr>
<tr><td>Invocación de influencias en el Estado</td><td>Cuando el servidor utiliza o simula su capacidad de influencia en el sector público para obtener un beneficio o una ventaja irregular.</td></tr>
<tr><td>Mantener intereses en conflicto</td><td>Cuando el servidor mantiene vínculos familiares, comerciales, institucionales o laborales que podrían afectar el manejo imparcial de los asuntos a su cargo y las relaciones de la entidad con actores externos.</td></tr>
<tr><td>Obstrucción al acceso a la información pública</td><td>Cuando el servidor se rehúsa a entregar información pública solicitada por los conductos regulares que no sea reservada, confidencial o secreta, de acuerdo con las normas vigentes.</td></tr>
<tr><td>Abuso de autoridad</td><td>Cuando el servidor comete u ordena un acto arbitrario alegando el cumplimiento de sus funciones.</td></tr>
<tr><td>Otro comportamiento</td><td>No previsto en los comportamientos descritos anteriormente.</td></tr>
</table></td></tr>
<tr><td>INTERACCIÓN O POTENCIAL AGENTE PRIMARIO</td><td>Aplica solo para el SGAS y MI.</td></tr>
<tr><td>18. POTENCIAL AGENTE PRIMARIO</td><td>Servidor público que forma parte de la unidad orgánica responsable del proceso sobre el cual se efectuará la identificación del riesgo. Cuenta con poder de decisión o influencia directa en la posible materialización del riesgo.</td></tr>
<tr><td>19. PARTES INTERESADAS RELACIONADAS O POTENCIALES AGENTES EXTERNOS (Aplicable solo al SGAS y MI)</td><td>Partes involucradas en el riesgo u oportunidad, considerando la matriz de partes interesadas. Aplicable solo al SGAS y MI.
Para el caso del MI, considerar actores externos a la entidad, incluyendo personas del sector público, privado o sociedad civil.</td></tr>
<tr><td>20. PUESTOS INVOLUCRADOS O POTENCIALES AGENTES INTERNOS (Aplicable solo al SGAS y MI)</td><td>Puestos involucrados en el riesgo u oportunidad. Aplicable solo al SGAS y MI.
Para el caso del MI, considerar actores internos de la entidad, que no pertenecen a la unidad orgánica responsable del proceso.</td></tr>
</table>

<table>
<tr><th>NUMERALES</th><th>DESCRIPCIÓN</th></tr>
<tr><td>21. PREGUNTAS DE VALIDACIÓN (Aplicable solo al MI)</td><td>Para establecer si se trata de un riesgo de corrupción o de inconducta funcional, se debe validar si se cumple(n) alguna(s) de las siguientes condiciones.

<table>
<tr><th>Preguntas de validación</th><th>Concepto</th></tr>
<tr><td>Ejercicio inadecuado de la función asignada al cargo</td><td>Existe un comportamiento irregular, por acción u omisión, vinculado a las funciones que ejerce el funcionario o servidor; es decir, se efectúa cuando la persona cumple o no cumple sus funciones.</td></tr>
<tr><td>Abuso del poder público</td><td>Existe un comportamiento irregular por el uso abusivo del poder que emana del cargo o la condición de ser funcionario o servidor público. La persona puede usar o acordar usar sus atribuciones o recursos, a los cuales tiene acceso, para acciones no vinculadas al ejercicio de sus funciones y fines distintos a los previstos.</td></tr>
<tr><td>Obtención de beneficio irregular o ventaja indebida para sí o para terceros</td><td>Existe un comportamiento irregular motivado por obtener un beneficio indebido (económico o no económico) o una ventaja (directa o indirecta), para sí o para terceros. No necesariamente implica un acuerdo con terceros; la persona puede actuar unilateralmente.</td></tr>
<tr><td>Perjuicio económico al Estado</td><td>Existe un comportamiento irregular que implica que el Estado pierde acceso (temporal o permanente) a recursos y/o existe defraudación patrimonial, como resultado de las acciones realizadas.</td></tr>
<tr><td>Incumplimiento explícito de norma o disposición legal</td><td>Existe una transgresión de deberes, prohibiciones, normas o disposiciones legales que pueden acarrear una responsabilidad a nivel administrativo, civil o penal, según corresponda.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">ANÁLISIS DE RIESGOS</td></tr>
<tr><td>22. MEDIDAS DE CONTROL EXISTENTES</td><td>Describir la o las medidas que se emplea actualmente para controlar o reducir el riesgo, así como detectar o aprovechar la oportunidad.
Antes de cada control, indicar el código del mismo, de la siguiente manera: "C + correlativo de dos dígitos" (Ejemplo: C01, C02, etc.)

Considerando la definición de control de la Norma ISO 31000:
<u>Control</u>:
Medida que mantiene y/o modifica un riesgo.
Nota 1 a la entrada: Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.
Nota 2 a la entrada: Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

Para los sistemas de gestión comprendidos en el SGIR se han considerado los siguientes controles:
• SGC: Controles de revisión, verificación y validación.</td></tr>
</table>

NUMERALES	DESCRIPCIÓN
	• SGAS: Controles financieros, no financieros y de debida diligencia. • SGSI: Cualquier acción tomada para gestionar el riesgo. • SCI: Cualquier acción tomada para gestionar el riesgo y aumentar las posibilidades de que los objetivos y metas se alcancen.
23. EFICACIA DE CONTROLES EXISTENTES	Indicar el nivel de los controles existentes, cuando sea aplicable.

Nivel de Eficacia	Definición	Definición aplicable al SGSI
Fuerte	Existen medidas de controles eficaces. Se efectúa periódicamente análisis y evaluaciones a los controles implementados para proponer mejoras y/o cambios a los mismos. Existe un nivel de documentación de su eficacia.	Existen medidas de control implementadas que han demostrado ser eficaces para mitigar el riesgo o aprovechar la oportunidad.
Moderado	Controles implementados. Existe un nivel de documentación básica, pero sin evidencia documental de su eficacia.	Existen medidas de control implementadas con eficacia media para mitigar el riesgo o aprovechar la oportunidad.
Débil	No se están aplicando controles o los controles implementados no son rigurosos o no documentados.	No existe medida de control alguna o el control existe es insuficiente o no riguroso para mitigar el riesgo o aprovechar la oportunidad.

24. PROBABILIDAD

Indicar la escala de la probabilidad de ocurrencia del riesgo **positivo** (Oportunidad).

Probabilidad	Valor	Definición	Frecuencia (Referencial)	% de Probabilidad
Muy Alto	5	La oportunidad tiene potencial de materializarse en la mayoría de las circunstancias	Más de 10 veces al año	80% - 100%
Alto	4	La oportunidad tiene potencial de materializarse con mucha frecuencia	De 5 a 9 veces al año	61% - 80%
Medio	3	La oportunidad tiene potencial de materializarse con poca frecuencia	De 2 a 4 veces al año	41% - 60%
Bajo	2	La oportunidad tiene potencial de materializarse con muy poca frecuencia	Al menos una vez en el último año	21% - 40%
Muy Bajo	1	La oportunidad tiene potencial de materializarse en circunstancias muy excepcionales	No se ha presentado en el último año	<20%

Indicar la escala de la probabilidad de ocurrencia del riesgo **negativo**.
Nota: el análisis de la probabilidad debe tomar en cuenta el o los controles existentes.

Probabilidad	Valor	Definición	Frecuencia (Referencial)	% de Probabilidad (Referencial)	Valor	Equivalencia SCI y MI Probabilidad
Muy Alto	5	El riesgo tiene potencial de materializarse en la mayoría de las circunstancias y el nivel de	Más de 10 veces al año	80% - 100%	10	**Muy Alta**

NUMERALES		DESCRIPCIÓN				
		eficacia de los controles existentes es débil.				
Alto	4	El riesgo tiene potencial de materializarse con mucha frecuencia y el nivel de eficacia de los controles existentes están entre débil y moderado.	De 5 a 9 veces al año	61% - 80%	8	**Alta**
Medio	3	El riesgo tiene potencial de materializarse con cierta frecuencia y el nivel de eficacia de los controles existentes están entre débil y moderado.	De 2 a 4 veces al año	41% - 60%	6	**Medio**
Bajo	2	El riesgo tiene potencial de materializarse con muy poca frecuencia y el nivel de eficacia de los controles existentes están entre moderados y fuerte.	Al menos una vez en el último año	21% - 40%	4	**Baja**
Muy Bajo	1	El nivel de eficacia de los controles existentes está entre moderados y fuertes por lo que mitigan el riesgo; o el riesgo por naturaleza tiene potencial de materializarse en circunstancias muy excepcionales, incluso sin controles implementados.	No se ha presentado en el último año	<20%		

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el riesgo identificado.
En caso de no contar con datos históricos, bajo el concepto de factibilidad se trabajará de acuerdo con el juicio experto de los servidores que desarrollan el proceso y de sus factores internos y externos.
Para el caso del MI, se aplica la siguiente regla:

- El riesgo de inconducta funcional tendrá como mínimo una probabilidad de ocurrencia media (pudiendo alcanzar una probabilidad alta o muy alta).
- El riesgo de corrupción tendrá como mínimo una probabilidad de ocurrencia alta (pudiendo alcanzar una probabilidad muy alta).

25. IMPACTO

Indicar la escala de impacto del riesgo **positivo** (Oportunidad).

Impacto Positivo	Valor	Definición
Altamente beneficioso	5	Es aquel riesgo que al presentarse puede generar grandes beneficios entre 16 al 20% para la Institución y el cumplimiento de los objetivos institucionales o del sistema de gestión o modelo en cuestión.
Mayor	4	Es aquel riesgo que al presentarse puede generar mayores beneficios entre 11 al 15 % para la Institución y el cumplimiento de los objetivos institucionales o del sistema de gestión o modelo en cuestión.
Moderado	3	Es aquel riesgo que al presentarse puede generar moderados beneficios entre 1 al 10 % para la Institución y el cumplimiento de los objetivos institucionales o del sistema de gestión o modelo en cuestión.
Menor	2	Es aquel riesgo que al presentarse genera oportunidades en la prestación del servicio de la Institución, las cuales no impacta en el cumplimiento de los objetivos institucionales o del sistema de gestión o modelo en cuestión.

NUMERALES		DESCRIPCIÓN
Insignificante	1	Es aquel riesgo que, al presentarse, su aprovechamiento no afecta sustancialmente los objetivos institucionales o del sistema de gestión o modelo en cuestión.

Indicar la escala de impacto del riesgo negativo.
Nota: el análisis del impacto debe tomar en cuenta el o los controles existentes.

Impacto Negativo	Valor	Definición	Consecuencias	Consecuencias cualitativas (Aplicable SGSI)	Valor	Equivalencia SCI y MI Impacto
Grave	5	Genera un grave impacto a la Institución.	Aquel riesgo que al presentarse causa una afectación del 81 al 100 % con respecto al logro de los objetivos institucionales.	Impacta en forma severa al punto de comprometer la confidencialidad, integridad o disponibilidad de activos de información críticos de la Institución o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables. El impacto se materializa sobre toda la Institución y su efecto se siente en todos los procesos y servicios.	10	**Muy Alto**
Mayor	4	Genera un mayor impacto a la Institución.	Aquel riesgo que al presentarse causa una afectación del 61 al 80 % con respecto al logro de los objetivos institucionales.	Impacta en forma considerable la confidencialidad, integridad o disponibilidad de activos de información de un proceso o servicio específico del OSITRAN, puede llegar a comprometer, paralizar o retrasar procesos claves de la entidad por un tiempo considerable.	8	**Alto**
Moderado	3	Genera un moderado impacto a la Institución.	Aquel riesgo que al presentarse causa una afectación del 41 a 60 % con respecto al logro	El impacto sobre la confidencialidad, integridad y disponibilidad del activo de información es limitado en tiempo y alcance. Afecta a un proceso de soporte o actividad específica y puede subsanarse en corto plazo.	6	**Medio**

NUMERALES			DESCRIPCIÓN			
			de los objetivos institucionales.			
Menor	2	Genera un menor impacto a la Institución.	Aquel riesgo que al presentarse causa una afectación del 21 al 40 % con respecto al logro de los objetivos institucionales.	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es leve y se puede solventar internamente, pues no afecta a un proceso o actividad específica.	4	**Bajo**
Insignificante	1	Genera impacto insignificante a la Institución.	Aquel riesgo que al presentarse causa una afectación del 0 al 20 % con respecto al logro de los objetivos institucionales.	El impacto sobre la confidencialidad, integridad y disponibilidad de los activos de información o procesos del alcance del SGSI es muy bajo.		

En la evaluación del impacto se considera a juicio experto la elección entre la columna definición y las consecuencias, eligiéndose el que resulte más aplicable para el tipo de riesgo en análisis.
Para el caso del MI, al estimar el impacto del riesgo se considera una escala con tres niveles (medio, alto y muy alto), tomando en cuenta el análisis de los posibles efectos del riesgo:

Escala de Impacto del Riesgo			
Categoría	**Valor**	**Condición**	**Efectos**
Media	6	La materialización del riesgo podría suponer uno de los cuatro efectos	1. Afectación de derechos de los públicos de interés. 2. Afectación de servicios. 3. Pérdida o desvío de recursos y bienes de la entidad. 4. Afectación del patrimonio o recursos de los usuarios.
Alta	8	La materialización del riesgo podría suponer de dos a cuatro efectos	
Muy alta	10	La materialización del riesgo podría suponer de dos a más efectos, incluyendo:	5. Posible interrupción de la actual gestión de la entidad.

26. NIVEL DEL RIESGO	Resultado de la multiplicación del valor de los numerales 24 y 25, según el Mapa de Calor.

Probabilidad		Impacto				
		Insignificante	Menor	Moderado	Mayor	Grave
		1	2	3	4	5
Muy Alto	5	Medio	Medio	Alto	Extremo	Extremo
Alto	4	Bajo	Medio	Alto	Alto	Extremo
Medio	3	Bajo	Medio	Medio	Alto	Alto
Bajo	2	Muy bajo	Bajo	Medio	Medio	Alto
Muy Bajo	1	Muy bajo	Muy bajo	Bajo	Bajo	Alto

NUMERALES	DESCRIPCIÓN

Aplicable solo al SCI en el marco de la Directiva N° 006-2019-CG/INTEG y sus modificatorias.

Probabilidad		Impacto			
		Bajo	Medio	Alto	Muy Alto
		4	6	8	10
Muy Alta	10	Medio	Alto	Extremo	Extremo
Alta	8	Medio	Alto	Alto	Extremo
Medio	6	Bajo	Medio	Alto	Alto
Baja	4	Bajo	Bajo	Medio	Medio

27. PRIORIZACIÓN

Aplicable sólo al SGSI.
La priorización de los riesgos se realiza utilizando una escala del 1 al 3, donde 1 es la máxima prioridad y 3 la última prioridad.
La prioridad será asignada considerando en primera instancia el nivel del riesgo (a mayor nivel de riesgo, mayor prioridad), sin embargo, ésta puede verse afectada por algunos factores, como los legales, operacionales y/o presupuestales, o juicio de experto.

Priorización
Prioridad 1
Prioridad 2
Prioridad 3

VALORACIÓN DEL RIESGO

28. TIPO DE RESPUESTA

Registrar tipo de respuesta que se dará ante el riesgo luego del análisis y evaluación (Ver tabla en numeral 26).

Tipo de respuesta	Definición
Aceptar	Cuando el riesgo/oportunidad se encuentre dentro de la línea de apetito, manteniendo las medidas de control existentes y revisándolas periódicamente. No limita la implementación de medidas de control propuestas.
Asumir	Cuando no cuente con la capacidad de mitigar el riesgo a un nivel aceptable y es necesario continuar con el desarrollo de la actividad, asumiendo las consecuencias de dicha decisión, manteniendo las medidas de control existentes y revisándolas periódicamente. No limita la evaluación de futuras acciones para mejorar la capacidad de respuesta al riesgo.
Evitar	Cuando no hay capacidad y no es necesario continuar con el desarrollo de la actividad.
Mitigar	Cuando la capacidad permite reducir la probabilidad o el impacto del riesgo.
Compartir	Cuando la capacidad permite la tercerización a fin de prevenir el riesgo.
Incrementar	Cuando la capacidad permite aumentar la probabilidad o el impacto para aprovechar la oportunidad.

Nivel de Riesgo con impacto NEGATIVO/ POSITIVO	Tipo de respuesta	Valor	Equivalencia SCI Nivel de Riesgo
Extremo	RIESGO: Asumir (*), Mitigar, Compartir o Evitar OPORTUNIDAD: Aceptar o Incrementar	80-100	**Muy Alto**
Alto	RIESGO: Asumir (*), Mitigar, Compartir o Evitar	48-64	**Alto**

NUMERALES	DESCRIPCIÓN		
	OPORTUNIDAD: Aceptar o Incrementar		
Medio	RIESGO: Asumir (*), Mitigar, Compartir o Evitar	32-40	**Medio**
	OPORTUNIDAD: Aceptar		
Bajo	RIESGO: Aceptar	16-24	Bajo
	OPORTUNIDAD: Aceptar		
Muy Bajo	RIESGO: Aceptar		
	OPORTUNIDAD: Aceptar		

(*) La línea de apetito al riesgo es hasta nivel bajo y la línea de apetito a la oportunidad es hasta nivel medio.
Para riesgos superiores a la línea de apetito, es necesario la evaluación de la amenaza versus uno o más de los siguientes factores: a) la capacidad de recursos y b) la capacidad de control que pueda tener Ositrán hacia ella.

TRATAMIENTO DEL RIESGO

29. MEDIDAS DE PREVENCIÓN O MITIGACIÓN (Aplicable solo al MI)

- Medidas de prevención, orientadas a evitar las causas del riesgo identificadas; buscan reducir la probabilidad de ocurrencia del riesgo.
- Medidas de mitigación, orientadas a mejorar la capacidad de respuesta de la entidad, en caso de materializarse el riesgo; buscan reducir el impacto.

Tipos de causas	Causas	Estrategias de Prevención
Causas Personales	• Predisposición por relación personal • Percepción de impunidad • Falta o deterioro de carácter ético • Desconocimiento	• Incrementar consciencia sobre las consecuencias • Optimizar el diseño organizacional (incluyendo medidas de carácter regulatorio y ajustes en los procesos) • Producir ajustes de comportamiento (incluyendo intervenciones de bajo costo, pautas éticas, entre otros)
Causas Organizacionales	• Alta discrecionalidad • Procesos ineficientes • Práctica normalizada • Presión jerárquica o de pares	

Efectos	Estrategias de Mitigación
• Pérdida o desvío de bienes o recursos de la entidad • Afectación del patrimonio o recursos de los usuarios	• Activar respuesta inmediata, a través de la aplicación de protocolos de actuación y gestión de crisis en casos de alta y muy alta gravedad. • Contener posibles efectos de mediano y largo plazo, a través del desarrollo de planes de

NUMERALES	DESCRIPCIÓN
	• Afectación de derechos o servicios • Afectación de la confianza de los públicos de interés • Continuidad de la actual gestión contingencia y procesos de mejora continua. • Demostrar acciones de debida diligencia, a través de generación de evidencia sobre la implementación de medidas de prevención.
30. MEDIDAS DE CONTROL PROPUESTOS	Registrar las actividades y/o controles a implementar según el "tipo de respuesta". Considerar como criterio la viabilidad (sobre la base de sus propios recursos).
31. CONTROLES ASOCIADOS A LA ISO 27001	Registrar el código del control del Anexo A vinculado a las medidas de control propuestas. Aplicable solo al SGSI.
32. MEDIO DE VERIFICACIÓN	Describir la evidencia de la medida de control propuesta.
33. RESPONSABLE DE IMPLEMENTACIÓN	Registrar responsables de implementación.
34. PLAZO DE INICIO	Registrar fecha de inicio de la implementación de la medida de control.
35. PLAZO DE TÉRMINO	Registrar fecha de término de la implementación de la medida de control.
DETERMINACIÓN DEL NIVEL DE RIESGO OBJETIVO	
36. PROBABILIDAD	Probabilidad objetivo (lo que se quiere lograr).
37. IMPACTO	Impacto objetivo.
38. NIVEL DE RIESGO	Nivel de Riesgo objetivo.
SEGUIMIENTO	
39. FRECUENCIA DE SEGUIMIENTO	Registrar la frecuencia (quincenal, mensual, trimestral, semestral o anual) de medición.
40. ESTADO DE LA IMPLEMENTACIÓN	

Registrar el estado según la siguiente tabla:

Tipo de respuesta	Definición
Implementado	Cuando la entidad ha cumplido con implementar la medida de control conforme la matriz de gestión integral de riesgos.
En Proceso	Cuando la entidad ha iniciado, pero aún no ha culminado con la implementación de la medida de control contenida en la matriz de gestión integral de riesgos.
Pendiente	Cuando la entidad no ha iniciado la implementación de la medida de control contenida en la matriz de gestión integral de riesgos.
No Implementado	Cuando la entidad no ha cumplido con implementar la medida de control contenida en la matriz de gestión integral de riesgos y la oportunidad para su ejecución ha culminado definitivamente.
No Aplicable	Aplicable solo al SCI. Cuando la medida de control contenida en la matriz de gestión integral de riesgos no puede ser ejecutada por factores no atribuibles a la entidad, debidamente sustentados, que imposibilitan su implementación.
Desestimado	Aplicable solo al SCI. Cuando la entidad decide no implementar la medida de control contenida en la matriz de gestión integral de riesgos, asumiendo las consecuencias de dicha decisión.

41. OBSERVACIÓN/ COMENTARIO	Registrar observaciones o comentarios respecto del riesgo o sus medidas o acciones propuestas.
REEVALUACIÓN DEL RIESGO (Después de implementada la medida de control)	

NUMERALES	DESCRIPCIÓN
42. PROBABILIDAD	Probabilidad, resultado de la reevaluación (después de vencido el plazo de implementación de los controles).
43. IMPACTO	Impacto resultado de la reevaluación.
44. NIVEL DEL RIESGO	Nivel de riesgo resultado de la reevaluación.
45. FECHA DE EVALUACIÓN DE EFICACIA	Registrar fecha de evaluación de eficacia de controles.
46. NIVEL DE EFICACIA	Resultado de la Comparación del Nivel de Riesgo reevaluado (numeral 44) versus Nivel de Riesgo objetivo (numeral 38). Registrar "SI" cuando el Nivel de Riesgo reevaluado es menor o igual a Nivel de Riesgo objetivo y se obtiene o disminuye la probabilidad objetivo. Registrar "NO" cuando el Nivel de Riesgo reevaluado es mayor que el Nivel de Riesgo objetivo o se incrementa la probabilidad objetivo.

Fuente: Elaboración propia

ANEXO N° 05

INVENTARIO DE CONTROLES EXISTENTES

1. CÓDIGO DEL RIESGO	2. RIESGO	3. CÓDIGO DEL CONTROL	4. MEDIDAS DE CONTROL EXISTENTES	5. TIPO DE CONTROL	6. FRECUENCIA DE EJECUCIÓN	7. RESPONSABLE	8. EVIDENCIA DE LA EJECUCIÓN	9. EVIDENCIA DEL CONTROL	10. DOCUMENTADO	11. EFECTIVIDAD DEL CONTROL

Fuente: Elaboración propia

DESCRIPCIÓN DEL INVENTARIO DE CONTROLES EXISTENTES

NUMERALES	DESCRIPCIÓN
1. CÓDIGO DEL RIESGO	Registrar OP si es oportunidad y RI si es riesgos, seguido de las siglas del sistema de gestión que corresponde, así como del código del proceso y la numeración correlativa en dos dígitos.
2. RIESGO	Describir las características generales o las formas en que se observa o manifiesta el riesgo u oportunidad. Para el caso del MI, el riesgo se redacta de la siguiente manera: *Agente(s) podría(n) [posible comportamiento irregular] en contexto de riesgo*.
3. CÓDIGO DEL CONTROL	Indicar el código, de la siguiente manera: "C + correlativo de dos dígitos" (Ejemplo: C01, C02, etc.)
4. MEDIDAS DE CONTROL EXISTENTES	Describir la o las medidas que se emplea actualmente para controlar o reducir el riesgo, así como detectar o aprovechar la oportunidad.
5. TIPO DE CONTROL	Utilizar los tipos de controles según sea el caso.

Tipo de Control	Descripción
Preventivo	Aquellos que sirven para reducir la probabilidad de ocurrencia o modificar la causa del riesgo. Se implementan antes de que ocurra un evento de riesgo, son los que sirven para evitar / prevenir el riesgo.
Detectivo	Sirven para detectar inconsistencias o generar alertas tempranas de que algo no está bien.
Correctivo	Aquellos que se implementan para mitigar el impacto causado por la materialización del riesgo. Se ejecutan durante o después de que este se presenta.

6. FRECUENCIA DE EJECUCIÓN	Registrar la frecuencia (quincenal, mensual, trimestral, semestral o anual) de ejecución.
7. RESPONSABLE	Registrar responsables de ejecutar la medida.
8. EVIDENCIA DEL CONTROL	Describir la evidencia de la medida de control existente.
9. DOCUMENTADO	Registrar "SI" cuando la evidencia del control sea documentada. Registrar "NO" cuando la evidencia del control no se documenta.

Fuente: Elaboración propia

ANEXO N° 06

MATRIZ DE COMUNICACIONES DEL SGIR

IT	QUE COMUNICA	CUANDO COMUNICA	A QUIÉN COMUNICA	CÓMO COMUNICA (Canales)	QUIÉN COMUNICA		EN QUÉ IDIOMAS COMUNICAR	TOMA DE CONCIENCIA PERIÓDICA
					RESPONSABLE	EJECUTA		
INTERNA								
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
EXTERNA								
1								
2								
3								
4								
5								

Fuente: Elaboración propia