RESOLUCIÓN DE GERENCIA GENERAL

N° 020-2022-GG-OSITRAN

Lima, 4 de marzo de 2022

VISTOS:

El Informe N° 021-2022-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto y el Memorando N° 0098-2022-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica y;

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 004-2016-PCM, de fecha 14 de enero de 2016, se aprobó el uso obligatorio de la NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición, la cual establece que la entidad debe evaluar y tratar los riesgos de seguridad de la información con la finalidad de proteger los activos de información;

Que, a través del Decreto Supremo N° 044-2018-PCM, de fecha 26 de abril de 2018, se aprobó el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021, que establece un modelo de integridad cuyo desarrollo corresponde a estándares internacionales y buenas prácticas planteadas desde la cooperación internacional con la finalidad de mejorar la organización de la administración pública para promover la integridad y luchar contra la corrupción. Este requerimiento normativo incorpora como uno de sus nueve componentes la gestión de los riesgos;

Que, por medio de la Resolución Directoral N° 014-2018-INACAL/DN, de fecha 04 de julio de 2018, se aprobó la NTP-ISO 31000:2018 Gestión del riesgo. Directrices. 2a Edición, que tiene por objetivo proporcionar directrices para gestionar el riesgo al que se enfrentan las organizaciones;

Que mediante Decreto Supremo N° 123-2018-PCM, de fecha 19 de diciembre de 2018, se aprobó el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública que señala que el Sistema Administrativo de Modernización de la Gestión Pública tiene por finalidad, entre otros, gestionar la evaluación de riesgos de gestión como mecanismo para contribuir al cumplimiento de los objetivos institucionales;

Que, a través de la Resolución de Contraloría N° 146-2019-CG, de fecha 17 de mayo de 2019 se aprobó la Directiva N° 006-2019-CG/INTEG “Implementación del Sistema de Control Interno en las Entidades del Estado”, que regula el procedimiento para implementar el Sistema de Control Interno (SCI) en las entidades del Estado y establece como uno de los ejes de dicho sistema, el Eje de Gestión de Riesgos;

Que, mediante Resolución de Secretaría de Integridad Pública N° 002-2021-PCM/SIP se aprobó la Directiva N° 002-2021-PCM/SIP “Lineamientos para fortalecer una cultura de integridad en las entidades del sector público”, que establece medidas de desempeño para el fortalecimiento de una cultura de integridad, desarrollando, entre otros, el componente de Gestión de Riesgos que afecten a la integridad pública;

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;

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

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 el Informe N° 021-2022-GPP-OSITRAN de fecha 03 de marzo de 2021, la Gerencia de Planeamiento y Presupuesto sustenta la necesidad de modificar el Manual de Gestión Integral de Riesgos;

Que, a través del Memorando N° 0098-2022-GAJ-OSITRAN de fecha 04 de marzo de 2021, la Gerencia de Asesoría Jurídica señaló que, considerando el sustento formulado por la Gerencia de Planeamiento y Presupuesto en el marco de sus competencias, resulta jurídicamente viable la aprobación de la modificación del Manual de Gestión Integral de Riesgos. Asimismo, indicó que en aplicación de la función prevista en el numeral 4 del artículo 11 del Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM y modificatorias, corresponde a la Gerencia General la aprobación de la modificación del Manual de Gestión Integral de Riesgos;

Que, según lo dispuesto en el artículo 11 del Reglamento de Organización y Funciones del Ositrán, aprobado mediante Decreto Supremo N° 012-2015-PCM y modificatorias, la Gerencia General es la máxima autoridad administrativa y tiene entre sus funciones la aprobación de 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;

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 la modificación del “Manual de Gestión Integral de Riesgos del Ositrán” y su versión actualizada, que como anexo forma parte integrante de la presente resolución.

Artículo 2.- Poner la presente Resolución en conocimiento de todas las unidades de organización del Ositrán, para difusión y aplicación.

Artículo 3.- Disponer la publicación de la presente resolución en el portal institucional de Ositrán (www.gob.pe/ositran).

Regístrese y comuníquese.

JUAN CARLOS MEJÍA CORNEJO
Gerente General

NT: 2022021140

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

Firmado por: LA ROSA ROSADO Victor Hugo FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 03/03/2022 14:00:16 -0500

Firmado por: MEJIA CORNEJO Juan Carlos FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 04/03/2022 18:56:58 -0500

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

MANUAL DE GESTIÓN INTEGRAL DE RIESGOS

VERSIÓN 02

Rol	Nombres y Apellidos	Cargo
Elaborado por:	Víctor Hugo La Rosa Rosado	Gerente de Planeamiento y Presupuesto
Revisado por:	Víctor Hugo La Rosa Rosado	Gerente de Planeamiento y Presupuesto
	Luis Miguel Torres Castillo	Jefe de Gestión de Recursos Humanos
	Eyleen Noriega Quiroz	Jefe de Tecnologías de la Información (e)
Aprobado por:	Juan Carlos Mejía Cornejo	Gerencia General

Visado por: NORIEGA QUIROZ Eyleen Carolina FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 03/03/2022 16:05:36 -0500

Visado por: TORRES CASTILLO Luis Miguel FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 03/03/2022 15:11:22 -0500

Visado por: BENITES RUIZ Paola Monica FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 03/03/2022 13:14:53 -0500

HOJA DE CONTROL DE CAMBIOS

Versión modificada	Descripción del Cambio
Versión 01	En el tercer párrafo del numeral 6.3.4.1 Identificación del riesgo: • Se modifica la identificación de riesgos desde el proceso nivel 1. En el Anexo 5 Matriz de Gestión Integral de Riesgos, en la matriz: • Se incorpora el Numeral 26 Controles asociados a la ISO 27001. • Se complementa en el Numeral 36 Observación el texto: Comentario. En la descripción de la matriz: • Se incorpora en el Numeral 9 Causa el texto: “No aplicable a SGSI, toda vez que la causa ya está expresada en términos de la vulnerabilidad y la amenaza”. • Se incorpora en el Numeral 20 Eficacia de controles existentes el texto: “cuando sea aplicable”. • Se complementa en el Numeral 24 Tipo de respuesta en la definición de Aceptar el texto: "manteniendo las medidas de control existentes y revisándolas periódicamente. No limita la implementación de medidas de control propuestas". • Se complementa en el Numeral 24 Tipo de respuesta en la definición de Asumir el texto: “manteniendo las medidas de control existentes y revisándolas periódicamente. No limita la evaluación de futuras acciones para mejorar la capacidad de respuesta al riesgo”. • Se incorpora el Numeral 26 Controles asociados a la ISO 27001 y la descripción: “Registrar el código del Anexo A vinculado a las medidas de control propuestas. Aplicable solo al SGSI”. • Se complementa en el Numeral 36 Observación el texto: “Comentario” y la descripción: “respecto del riesgo o sus medidas o acciones propuestas”.

ÍNDICE

I. OBJETIVO

Establecer 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.

II. FINALIDAD

Contribuir con la construcción 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, 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, publicada en el Diario Oficial “El Peruano” el 17.05.19 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/RT-ISO/TR 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 Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.
- 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 9001:2015 Sistemas de gestión de la calidad. Requisitos. 6ª Edición.

V. CONTENIDO GENERAL

5.1 OBJETIVOS DE LA GESTIÓN INTEGRAL DEL RIESGO

- Aumentar la probabilidad de alcanzar los objetivos de la entidad.
- Ser consciente 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.
- Cumplir con la normativa aplicable.

- Contribuir con mejorar 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.
- Mejorar la eficacia y eficiencia operativa.
- Mejorar el aprendizaje y la flexibilidad organizacional.

5.2 POLÍTICA INSTITUCIONAL DE LA GESTIÓN INTEGRAL DEL RIESGO

La Presidencia Ejecutiva define la Política Institucional de la Gestión Integral de Riesgos. Dicha política debe ser comunicada dentro de la entidad y encontrarse disponible para las partes interesadas y de cumplimiento para todos los servidores civiles, independiente de su modalidad de contratación.

5.2.1. OBJETIVO DE LA POLÍTICA

Establecer el compromiso y los lineamientos generales sobre los cuales se efectuará la Gestión Integral de Riesgos en el Ositrán.

5.2.2. FINALIDAD DE LA POLÍTICA

Incrementar la probabilidad del logro de los objetivos estratégicos, a través de la reducción de la incertidumbre, anticipación, gestión y control de los riesgos a los que están expuestos los procesos del Ositrán, haciendo frente a las consecuencias en caso estos se materialicen.

Somos conscientes que, producto del contexto en el que realizamos nuestras actividades, podemos identificar oportunidades que generen efectos positivos en el logro de los objetivos, y siempre y cuando sea factible, las aprovecharemos.

5.2.3. COMPROMISO

Ositrán, alineado con su visión, misión y valores, manifiesta su compromiso con la integración, diseño, implementación, seguimiento y mejora de su SGIR, a fin de detectar, controlar y hacer frente a posibles eventos que tuvieran impacto sobre el logro de los objetivos de la entidad.

Asimismo, la Alta Dirección se compromete a asignar los recursos para la implementación de la Gestión Integral de Riesgos en la entidad.

5.2.4. ALCANCE DEL SISTEMA DE GESTIÓN INTEGRAL DE RIESGOS

La Política Institucional de Gestión Integral de Riesgos abarca a todas las unidades de organización del Ositrán, sus funciones, procesos y actividades, debiendo ser aplicada por los servidores civiles de acuerdo con sus responsabilidades, ejecutando la metodología, procedimientos y herramientas establecidas en el marco del SGIR.

5.2.5. LINEAMIENTOS PARA LA GESTIÓN INTEGRAL DEL RIESGO

a. La Gestión Integral de Riesgos se alinea a la estrategia del Ositrán y se incorpora en las funciones, procesos y actividades de la entidad.
b. Comprende la planificación, identificación, análisis, valoración y tratamiento de los riesgos; así como la gestión de registros e informes, comunicación y consulta, además del seguimiento y revisión.
c. Los riesgos deben medirse en función de su probabilidad de ocurrencia y el impacto sobre los objetivos y resultados de la entidad.

d. El Ositrán promueve la cultura de Gestión Integral de Riesgos en todas las unidades de organización.
e. Todas las unidades de organización son responsables de aplicar en sus funciones, procesos y actividades, la metodología, procedimientos y herramientas que se desarrollen como parte de la Gestión Integral de Riesgos, de acuerdo con el ámbito de su competencia.
f. La metodología de la Gestión Integral de Riesgos deberá precisar la línea del apetito al riesgo que asumirá la entidad.
g. La Política Institucional de la Gestión Integral de Riesgos debe ser revisada periódicamente para garantizar la continuidad de la Gestión Integral de Riesgos.

5.3 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 está compuesto por el:

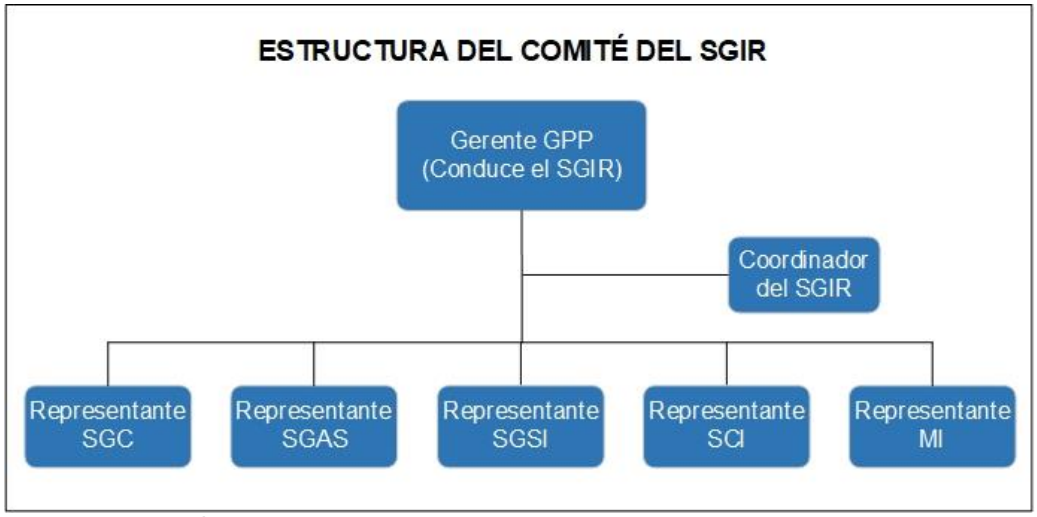
- Presidente Ejecutivo.

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 el:

- Gerente General, quien lo preside.
- Gerente de Administración.
- Gerente de Supervisión y Fiscalización.
- Gerente de Planeamiento y Presupuesto.

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

- Gerente de Planeamiento y Presupuesto, quien lo conduce.
- Un representante del SGC.
- Un representante del SGAS.
- 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 del riesgo 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 enfrenta sus procesos/productos.

Los Responsables de implementación tienen la responsabilidad de implementar las medidas de control propuestas para mitigar los riesgos.

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

En el Anexo N° 03, se detallan los roles y responsabilidades del SGIR.

VI. CONTENIDO ESPECIFÍCO

6.1 CONCEPTOS BASICOS

Basados en la Norma ISO 31000:2018 - Guía 73 Basada 31100

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 contenido 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 la tecnología de información, a la comunicación y a eventos externos. También se consideran riesgos que afecten los activos de información a proteger.

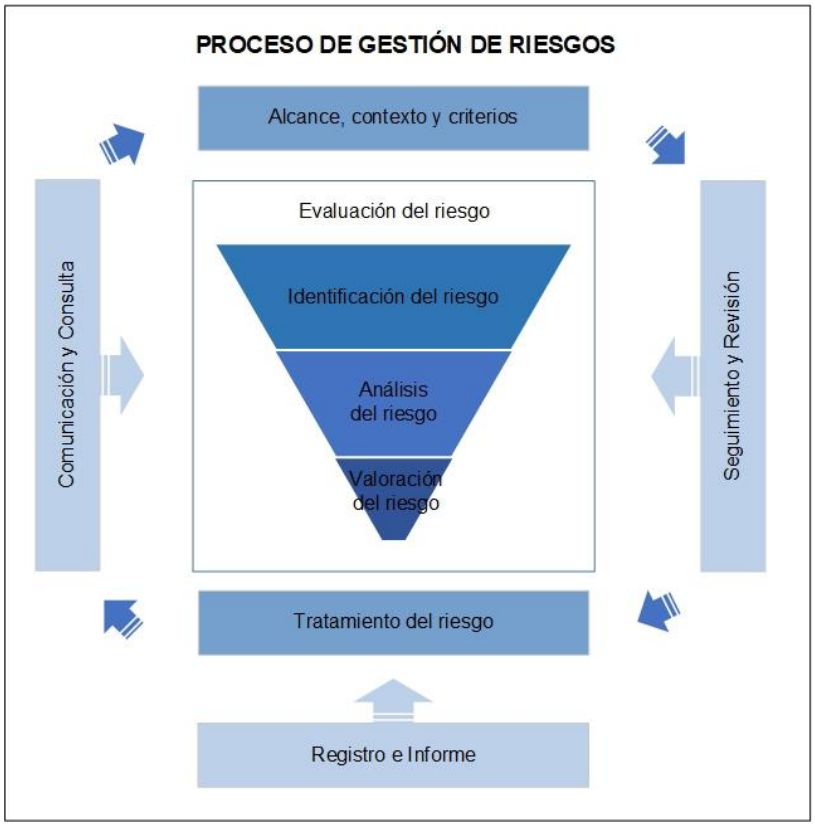
Tipos de Riesgos	Concepto
Financiero	El riesgo financiero está asociado a los riesgos de liquidez y solvencia. Está relacionado con eventos que afecten la gestión de los recursos financieros de la institución y el financiamiento de sus operaciones, siempre que no hayan sido causados directamente por 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 Corrupción	Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
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].

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* y el marco integrado de Control Interno de la Contraloría General de la República, basado en el COSO.

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 según el estándar ISO 31000.



[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 de los entornos 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.

En el Anexo N° 04 se describe los aspectos externos e internos que se debe considerar como mínimo para el establecimiento del contexto.

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 que se encuentran certificadas o en proceso de implementación, 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 y tratamiento del riesgo, según el Anexo N° 05.

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

La GG remitirá mediante memorando circular la Matriz de Gestión Integral de Riesgos firmada a las unidades de organización para conocimiento y a la JGRH para su publicación en la intranet institucional en coordinación con la GPP.

6.3.3 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 tratamientos 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 riesgos de seguridad de la información, se debe considerar los activos de información identificados previamente en la "Matriz de Inventario de Activos de Información".

El registro de la identificación del riesgo se realiza 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
- Efectos o consecuencias
- Descripción del riesgo/oportunidad
- Tipo de riesgo
- Dueño del riego
- Código del riesgo
- Tipo de sistema de gestión
- Partes interesadas relacionadas
- Puestos involucrados

En el Anexo N° 05 se detalla la descripción de los criterios para la identificación del riesgo.

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

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 y que se tenga capacidad de gestionar.
  ¿Qué ocasionó u ocasionaría dicho riesgo? Ese origen debe ser algo que el Ositrán tiene capacidad de gestionar.

- 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 el 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 calificación por cada medida de control existente con respecto a las características de su diseño y la eficacia del mismo, ver numeral 20 de la descripción de la Matriz, según el Anexo N° 05.

La unidad de organización debe analizar la probabilidad de ocurrencia del riesgo y del impacto de su materialización en la entidad; para este análisis se utiliza los numerales 21 y 22 de la descripción de la Matriz, según el Anexo N° 05.

A partir de la determinación de la probabilidad de ocurrencia del riesgo y su nivel de impacto, se determina el nivel de riesgo, ver numeral 23 de la descripción de la Matriz, según el Anexo N° 05.

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].

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

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 hacia ella
c. La intención de hacer daño

En el numeral 24 de la descripción de la Matriz se detalla los tipos de respuesta para el tratamiento del riesgo, según el Anexo N° 05.

6.3.5 TRATAMIENTO DEL RIESGO

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

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) y factibles.

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.

El registro del tratamiento del riesgo se realiza 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

A partir del tratamiento del riesgo, se determina el nivel de riesgo objetivo, para lo cual se establece la probabilidad de ocurrencia del riesgo que se desea lograr y el impacto de su concreción en la entidad, ver numerales 31, 32 y 33 de la descripción de la Matriz, según el Anexo N° 05.

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].

La GPP establece la frecuencia del seguimiento de la implementación de las medidas de control propuestas, acorde a los plazos definidos de inicio y fin, en coordinación el responsable de la implementación. Ver numeral 34 de la descripción de la Matriz, según el Anexo N° 05.

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

[6] Numeral 6.4.5 ISO 31000: 2018
[7] Numeral 6.6 ISO 31000: 2018

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

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 tratados mediante las medidas de control propuestas, aplicando para ello, los numerales 37, 38 y 39 de la descripción de la Matriz, según el Anexo N° 05.

Cuando la unidad de organización determine 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.

A partir de reevaluación del riesgo, la unidad de organización determina el nivel de eficacia comparando el nivel de riesgo identificado con el nivel de riesgo reevaluado y registra "Si", cuando el control fue eficaz y "No" cuando el control no fue eficaz, ver numeral 41 de la descripción de la Matriz, según el Anexo N° 05.

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].

[8] Numeral 6.2 ISO 31000: 2018

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.

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.

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.

A partir de ello, los Coordinadores del SGIR de cada sistema de gestión y modelo consolidan la información y elaboran un reporte semestral para ser remitido al Comité del SGIR.

[9] Numeral 6.7 ISO 31000: 2018

El Coordinador del Comité del SGIR revisa los reportes sobre los avances de la ejecución de las medidas de control propuestas 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 semestral.

VII. ANEXOS

Anexo N° 01:	ACRÓNIMOS
Anexo N° 02:	GLOSARIO DE TERMINOS
Anexo N° 03:	ROLES Y RESPONSABLES DEL SGIR
Anexo N° 04:	ESTABLECIMIENTO DEL CONTEXTO EXTERNO E INTERNO
Anexo N° 05:	MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS
Anexo N° 06:	MATRIZ DE COMUNICACIONES DEL SGIR

ANEXO N° 01

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
SGI	:	Sistema Integrado de Gestión
SGIR	:	Sistema de Gestión Integral de Riesgos
SGSI	:	Sistema de Gestión de Seguridad de la Información

ANEXO N° 02

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.
- Factible: Posible, que puede hacerse o realizarse.
- Medida de control existente: Medida que se emplea actualmente para controlar o reducir el riesgo o detectar la oportunidad.
- 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.
- 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.
- 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: Que puede ser realizado.

ANEXO N° 03

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° 04

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	Conocimiento del funcionamiento del Sistema de Gestión y Modelo.
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 Guía para el proceso de Comunicación Interna[12].

[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.
[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.

Aspectos Internos	Descripción
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

ANEXO N° 05

MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

ÁREA / PROCESO / SUB PROCESO / OBJETIVO / ACTIVO						IDENTIFICACIÓN														ANÁLISIS					VALORACIÓN	TRATAMIENTO								SEGUIMIENTO			REEVALUACIÓN DEL RIESGO (Después de implementada la medida de control)				
						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. OPORTUNIDAD / AMENAZA	8. FORTALEZA / DEBILIDAD / VULNERABILIDAD	9. CAUSA	10. RIESGO/ OPORTUNIDAD IDENTIFICADO	11. EFECTO O CONSECUENCIA	12. RIESGO U OPORTUNIDAD	13. TIPO DE RIESGO	14. DUEÑO DEL RIESGO	15. CODIGO	SGC	SGAS	SGSI	SCI	MI	17. PARTES INTERESADAS RELACIONADAS	18. PUESTOS INVOLUCRADOS	19. MEDIDAS DE CONTROL EXISTENTES	20. EFICACIA DE MEDIDAS DE CONTROL EXISTENTES	21. PROBABILIDAD (P)	22. IMPACTO (I)	23. NIVEL DE RIESGO (NR)	24. TIPO DE RESPUESTA	25. MEDIDAS DE CONTROL PROPUESTOS	26. CONTROLES ASOCIADOS A LA ISO 27001	27. MEDIO DE VERIFICACIÓN	28. RESPONSABLE DE IMPLEMENTACIÓN	29. FECHA DE INICIO	30. FECHA DE TÉRMINO	31. PROBABILIDAD (P)	32. IMPACTO (I)	33. NIVEL DEL RIESGO (NR)	34. FRECUENCIA DE SEGUIMIENTO	35. ESTADO DE LA IMPLEMENTACIÓN	36. OBSERVACIÓN/ COMENTARIO	37.PROBABILIDAD (P)	38. IMPACTO (I)	39. NIVEL DEL RIESGO (NR)	40. FECHA DE EVALUACIÓN DE	41. EFICACIA

Fuente: Elaboración propia

DESCRIPCIÓN DE LA MATRIZ DE GESTIÓN INTEGRAL DE RIESGOS

NUMERALES	DESCRIPCIÓN
ÁREA/PROCESO/SUB PROCESO	
1. ÓRGANO/UNIDAD ORGÁNICA/OFICINA/ÁREA	Indicar el órgano, unidad orgánica, oficina o área al que pertenece el proceso.
2. PROCESO	Registrar el proceso que puede verse afectado.
3. SUBPROCESO	Registrar el subproceso que puede verse afectado, tomando en cuenta el de menor nivel.
4. OBJETIVO	Registrar la razón de ser del subproceso/proceso, tomando en cuenta el de menor nivel.
5. ACTIVO	Registrar el nombre del activo crítico sobre la base de la matriz de inventarios activos de información. Aplicable solo al SGSI.
6. PRODUCTO PRIORIZADO	Registrar el producto priorizado que puede verse afectado, en caso corresponda. Aplicable solo al SCI.
IDENTIFICACIÓN DEL RIESGO	
7. OPORTUNIDAD/AMENAZA	Registrar la Oportunidad o Amenaza que podría afectar el logro de los objetivos, asociada con el numeral 4.
8. FORTALEZA/DEBILIDAD/ VULNERABILIDAD	Registrar Fortaleza o Debilidad o vulnerabilidad, asociada con el numeral 7.
9. CAUSA	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.
10. RIESGO U OPORTUNIDAD	Registrar si se considera un riesgo (negativo) o una oportunidad (positivo).
11. EFECTO O CONSECUENCIA	Describir el impacto que podría generar el riesgo u oportunidad con respecto a los objetivos.
12. RIESGO/OPORTUNIDAD IDENTIFICADO	Describir las características generales o las formas en que se observa o manifiesta el riesgo u oportunidad.
13. TIPOS DE RIESGOS	Utilizar los tipos de riesgos según sea el caso.

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. También se consideran riesgos que afecten los activos de información a proteger. 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 Corrupción	Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
De Imagen	Asociados con la percepción y la confianza de las partes interesadas hacia la institución.

14. DUEÑO DEL RIESGO	Registrar la Unidad de organización que rinde cuentas del desempeño de sus riesgos.

NUMERALES	DESCRIPCIÓN
15. CÓDIGO	Registrar OP si es oportunidad y RI si es riesgos, además de 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 SGI (Seguridad de la Información) o SCI (Control Interno) o MI (Modelo de Integridad). Para el caso del MI, consignar el tipo de delito según sea el caso: • MI-Peculado • MI-Colusión • MI-Malversación de fondos • MI-Tráfico de Influencias • MI-Enriquecimiento Ilícito • MI-Concusión • MI-Negociación Incompatible • MI-Integridad y Ética
INTERACCIÓN	Aplica solo al SGAS y MI.
17. PARTES INTERESADAS RELACIONADAS	Partes involucradas en el riesgo u oportunidad, considerando la matriz de partes interesadas. Aplicable solo al SGAS y MI.
18. PUESTOS INVOLUCRADOS	Puestos involucrados en el riesgo u oportunidad. Aplicable solo al SGAS y MI.
ANÁLISIS DE RIESGOS	
19. MEDIDAS DE CONTROL EXISTENTES	Describir la medida que se emplea actualmente para controlar o reducir el riesgo, así como detectar la oportunidad. Considerando la definición de control de la Norma ISO 31000: 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. Para los sistemas de gestión comprendidos en el SGIR se han considerado los siguientes controles: • SGC: Controles de revisión, verificación y validación. • SGAS: Controles financieros, no financieros y de debida diligencia. • SGSI: Controles declarados en el Anexo A de la Norma ISO 27001:2013 • SCI: Cualquier acción tomada para gestionar el riesgo y aumentar las posibilidades de que los objetivos y metas se alcancen.
20. EFICACIA DE CONTROLES EXISTENTES	Indicar el nivel de los controles existentes, cuando sea aplicable.

NUMERALES	DESCRIPCIÓN

Nivel de Eficacia	Definición
Fuerte	Existen medidas de controles eficaces y eficientes. Se efectúa periódicamente análisis y evaluaciones a los controles implementados para proponer mejoras y/o cambios a los mismos.
Moderado	Controles implementados. Existe un nivel de documentación básica, pero sin evidencia documental de su eficacia.
Débil	No se están aplicando controles o los controles implementados no son rigurosos o no documentados.

21. PROBABILIDAD

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

Probabilidad	Valor	Definición	Frecuencia	% de Probabilidad
Muy Alto	5	El riesgo tiene potencial de materializarse en la mayoría de las circunstancias	Más de 10 veces al año	80% - 100%
Alto	4	El riesgo tiene potencial de materializarse con mucha frecuencia	De 5 a 9 veces al año	61% - 80%
Medio	3	El riesgo tiene potencial de materializarse con poca frecuencia	De 2 a 4 veces al año	41% - 60%
Bajo	2	El riesgo tiene potencial de materializarse con muy poca frecuencia	Al menos una vez en el último año	21% - 40%
Muy Bajo	1	El riesgo 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**.

Probabilidad	Valor	Definición	Frecuencia	% de Probabilidad	Valor	Equivalencia SCI Probabilidad
Muy Alto	5	El riesgo tiene potencial de materializarse en la mayoría de las circunstancias	Más de 10 veces al año	80% - 100%	10	**Muy Alta**
Alto	4	El riesgo tiene potencial de materializarse con mucha frecuencia	De 5 a 9 veces al año	61% - 80%	8	**Alta**
Medio	3	El riesgo tiene potencial de materializarse con poca frecuencia	De 2 a 4 veces al año	41% - 60%	6	**Medio**
Bajo	2	El riesgo tiene potencial de materializarse con muy poca frecuencia	Al menos una vez en el último año	21% - 40%	4	**Baja**
Muy Bajo	1	El riesgo tiene potencial de materializarse en circunstancias muy excepcionales	No se ha presentado en el último año	<20%		

NUMERALES	DESCRIPCIÓN
22. 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.
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.
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.
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.
Insignificante	1	Es aquel riesgo que, al presentarse, su aprovechamiento no afecta sustancialmente los objetivos institucionales.

Indicar la escala de impacto del riesgo **negativo**.

Impacto Negativo	Valor	Definición	Frecuencia	Valor	Equivalencia SCI 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.	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.	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 de los objetivos institucionales.	6	**Medio**
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.	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.		

23. NIVEL DEL RIESGO	Resultado de la multiplicación del valor de los numerales 21 y 22, 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

NUMERALES		DESCRIPCIÓN				
Muy Bajo	1	Muy bajo	Muy bajo	Bajo	Bajo	Alto

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 OPORTUNIDAD: Aceptar o Incrementar	48-64	Alto
Medio	RIESGO: Asumir (*), Mitigar, Compartir o Evitar OPORTUNIDAD: Aceptar	32-40	Medio
Bajo	RIESGO: Aceptar OPORTUNIDAD: Aceptar	16-24	Bajo
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, b) la capacidad de control que pueda tener Ositrán hacia ella, y c) la intención de hacer daño.

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

VALORACIÓN DEL RIESGO

24. TIPO DE RESPUESTA

Registrar tipo de respuesta que se dará ante el riesgo luego del análisis y evaluación (Ver tabla en numeral 23).

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.

NUMERALES	DESCRIPCIÓN
Incrementar	Cuando la capacidad permite aumentar la probabilidad o el impacto para aprovechar la oportunidad.

TRATAMIENTO DEL RIESGO	
25. 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).
26. CONTROLES ASOCIADOS A LA ISO 27001	Registrar el código del Anexo A vinculado a las medidas de control propuestas. Aplicable solo al SGSI.
27. MEDIO DE VERIFICACIÓN	Describir la evidencia de la medida de control propuesta.
28. RESPONSABLE DE IMPLEMENTACIÓN	Registrar responsables de implementación.
29. PLAZO DE INICIO	Registrar fecha de inicio de la implementación de la medida de control.
30. PLAZO DE TÉRMINO	Registrar fecha de término de la implementación de la medida de control.
DETERMINACIÓN DEL NIVEL DE RIESGO OBJETIVO	
31. PROBABILIDAD	Probabilidad objetivo (lo que se quiere lograr).
32. IMPACTO	Impacto objetivo.
33. NIVEL DE RIESGO	Nivel de Riesgo objetivo.
SEGUIMIENTO	
34. FRECUENCIA DE SEGUIMIENTO	Registrar la frecuencia (quincenal, mensual, trimestral, semestral o anual) de medición.
35. 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.

36. 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)	
37. PROBABILIDAD	Probabilidad, resultado de la reevaluación (después de vencido el plazo de implementación de los controles).
38. IMPACTO	Impacto resultado de la reevaluación.
39. NIVEL DEL RIESGO	Nivel de riesgo resultado de la reevaluación.

NUMERALES	DESCRIPCIÓN
40. FECHA DE EVALUACIÓN DE EFICACIA	Registrar fecha de evaluación de eficacia de controles.
41. NIVEL DE EFICACIA	Resultado de la Comparación del Nivel de Riesgo objetivo (numeral 33) versus Nivel de Riesgo reevaluado (numeral 39). Registrar "SI" si el control fue eficaz y "NO" si el control no fue eficaz.

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