GABRIELA BERTHA HERRERA TAN
Secretaria General
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: HERRERA TAN Gabriela Bertha FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 12/01/2026 16:15:15-0500

Lima, 12 de Enero del 2026

RESOLUCION SECRETARIAL N° 000004-2026/SGEN/RENIEC

VISTOS:

Los Memorandos N° 001081-2025/OILCC/RENIEC (12DIC2025) y Nº 001100-2025/OILCC/RENIEC (17DIC2025) de la Oficina de Integridad y Lucha contra la Corrupción, el Informe Nº 000025-2025/FCH/OILCC/FCARO/RENIEC (12DIC2025) del Supervisor de la Oficina de Integridad y Lucha contra la Corrupción; el Memorando Nº 000018-2026/OPPM/RENIEC (09ENE2026) de la Oficina de Planeamiento, Presupuesto y Modernización; el Informe N° 000004-2026/OPPM/UMO/RENIEC (09ENE2026) de la Unidad de Modernización Organizacional de la Oficina de Planeamiento, Presupuesto y Modernización; el Informe Nº 000029-2026/OAJ/RENIEC (12ENE2026) de la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que por la Ley Nº 26497 se creó el Registro Nacional de Identificación y Estado Civil (RENIEC), con arreglo a los artículos 177º y 183º de la Constitución Política del Perú, como organismo constitucionalmente autónomo, con personería jurídica de derecho público interno, que goza de atribuciones en materia registral, técnica, administrativa, económica y financiera, encargado entre otros, de manera exclusiva y excluyente de organizar y actualizar el Registro Único de Identificación de las Personas Naturales, así como de inscribir los hechos y actos relativos a su capacidad y estado civil;

Que mediante la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, se establece como finalidad fundamental del proceso de modernización, la obtención de mayores niveles de eficiencia del aparato estatal, con el objetivo de alcanzar, entre otros, un Estado transparente en su gestión, con trabajadores y servidores que brindan al ciudadano un servicio imparcial, oportuno, confiable, predecible y de bajo costo, lo que implica el desempeño responsable y transparente de la función pública, con mecanismos de control efectivos;

Que de igual forma, el Decreto Supremo N° 103-2022-PCM que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030, precisa como objetivos prioritarios el de “Garantizar políticas públicas que respondan a las necesidades y expectativas de las personas en el territorio”, el de “Mejorar la gestión interna en las entidades públicas”, el de “Fortalecer la mejora continua en el Estado” y el de “Garantizar un gobierno abierto que genere legitimidad en las intervenciones públicas”;

Que la Ley N° 28716, Ley de Control Interno de las entidades del Estado, tiene como propósito de cautelar y fortalecer los sistemas administrativos con acciones y actividades de control previo, simultáneo y posterior; en concordancia con la Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno con el objetivo principal de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública; y, la Resolución de Contraloría N° 0146-2019-CG, que aprueba la Directiva N° 006-2019-CG-INTEG sobre "Implementación del Sistema de Control Interno en las Entidades del Estado", como precepto regulador del procedimiento para implementar el Sistema de Control Interno en las entidades del Estado, así como las normas que dicten los órganos rectores de los sistemas administrativos;

Que los diversos órganos y unidades orgánicas del RENIEC, en su constante compromiso de mejoramiento, vienen revisando su normativa, a efecto de solicitar la aprobación de nuevos documentos normativos o Información Documentada, o en otros casos éstos se dejen sin efecto, con la finalidad de mejorar u optimizar las labores de cada una de ellas;

Que mediante Informe Nº 000025-2025/FCH/OILCC/FCARO/RENIEC (12DIC2025) del Supervisor de la Oficina de Integridad y Lucha contra la Corrupción y Memorando N° 001081-2025/OILCC/RENIEC (12DIC2025), la Oficina de Integridad y Lucha contra la Corrupción, propone la aprobación del proyecto de Información Documentada Manual "Gestión Integral Del Riesgo", Primera Versión, señalando que tiene por objeto y aplicación identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos institucionales, las disposiciones legales y normativas del Estado, especialmente aquellos vinculados con la integridad pública, la seguridad de la información, la calidad del servicio y la confianza ciudadana. Dicho enfoque busca anticiparse a posibles eventos que puedan comprometer la transparencia, la eficiencia y eficacia en el otorgamiento de productos y prestación de servicios. Asimismo, su aplicación permite integrar otros sistemas de gestión reconocidos, como el de gestión de la calidad ISO 9001, seguridad de la información ISO 27001, sistema de gestión antisoborno ISO 37001, o cualquier otro sistema de gestión basado en el ciclo de mejora continua;

Que la Oficina de Integridad y Lucha contra la Corrupción sustenta su propuesta de Información Documentada en:

La 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", mediante la que se establecen medidas de desempeño para el fortalecimiento de una cultura de integridad en las entidades de la Administración Pública, y uno de los componentes del modelo de integridad es la "Gestión de riesgos que afectan la integridad pública;

La 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", con la finalidad de desarrollar pautas generales para la gestión de riesgos que afectan la integridad pública, a fin de orientar a las entidades del Estado en el proceso de implementación del componente de Gestión de Riesgos del Modelo de Integridad establecido para las entidades del sector público;

La Directiva N° 001-2024-PCM/SIP "Directiva para la incorporación y ejercicio de la función de integridad en las entidades de la administración pública" aprobada por Resolución de Secretaría de Integridad Pública 001-2024-PCM/SIP, la misma que entre otras funciones de la Unidad de Organización que ejerce la función de integridad, en relación a la gestión de riesgos establece las siguientes funciones:

"(…)

e) Conducir la gestión de riesgos que afectan la integridad pública, en coordinación con la máxima autoridad administrativa y los órganos y unidades orgánicas de la entidad; conducir y dirigir la estrategia institucional de integridad y lucha contra la corrupción, así como supervisar su cumplimiento.

(…)

La Resolución de Secretaría de Gestión Pública N° 002-2025-PCM-SGP que aprueba la Norma Técnica N° 002-2025-PCM/SGP, Norma Técnica para la Gestión por Procesos en las entidades de la Administración Pública, en la cual establecen que los riesgos, son elementos del proceso, y se refieren a las situaciones que pueden generar desvíos en el cumplimiento de los objetivos del proceso para la entrega de productos, por tal motivo es importante identificarlos;

La Resolución Directoral N° 014-2018-INACAL/DN, que aprueba normas técnicas, entre las que se encuentra la NTP-ISO 31000:2018 Gestión del Riesgo. Directrices, 2a Edición, que nos brinda las pautas y orientaciones para implementar y mejorar de manera continua una estructura para la gestión del riesgo, con la finalidad de asegurar que el riesgo se gestione de manera coherente y consistente, mejorando la toma de decisiones informadas al asegurar que las incertidumbres asociadas a los objetivos estratégicos de la entidad se consideren de manera explícita y profesional;

Que asimismo, mediante Memorando Nº 001100-2025/OILCC/RENIEC (17DIC2025) la Oficina de Integridad y Lucha contra la Corrupción señala que el proyecto de Información Documentada denominado Manual de Gestión Integral del Riesgo, Primera Versión, tiene como base las pautas directrices metodológicas de la ISO 31000:2018 Gestión del Riesgo Directrices, la misma que no es un sistema de gestión (SG) certificable como otras normas (ej. ISO 9001) porque no define requisitos para un SG específico, sino que ofrece directrices y principios generales para integrar la gestión de riesgos, actuando como un marco flexible y no prescriptivo para mejorar la toma de decisiones, en ese sentido solicita mantener la denominación como Manual de Gestión Integral del Riesgo; solicitando asimismo que previo a la aprobación del Manual, se deje sin efecto la Directiva DI-010-OIR/002 “Gestión Integral del Riesgo”, primera versión, aprobada mediante Resolución Secretarial Nº 000004-2023/SGEN/RENIEC (09ENE2023) y el Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, segunda versión, aprobado mediante Resolución Secretarial Nº 000029-2020/SGEN/RENIEC (04JUN2020);

Que a través de la Resolución Jefatural Nº 000061-2024/JNAC/RENIEC (08ABR2024) y publicada en el Diario Oficial El Peruano el 11ABR2024, se aprobó el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, el cual ha dispuesto cambios sustanciales en la organización y funciones de diversos órganos y unidades orgánicas, lo que involucra la necesidad de actualizar, entre otros, los documentos normativos y la Información Documentada, que regulan las actividades al interior de la administración;

Que el numeral 6 de la Guía de Procedimientos GP-001-OPPM/UMO/001, denominada “Información Documentada del RENIEC”, primera versión, aprobada con Resolución Secretarial N° 000109-2024/SGEN/RENIEC (19SET2024), en su articulado regula la formulación, revisión, aprobación y derogación de la Información Documentada, entre otros aspectos;

Que el numeral 7.6 de la Directiva DI-001-OPPM/001 “Documentos Normativos del RENIEC”, primera versión, aprobada por la Resolución Secretarial N° 000084-2024/SGEN/RENIEC (08JUL2024), regula los lineamientos para la derogación de los documentos normativos, entre otros aspectos;

Que en esa línea, es preciso señalar que la Unidad de Modernización Organizacional de la Oficina de Planeamiento, Presupuesto y Modernización, en su condición de órgano técnico especializado de la Institución, determinó que el proyecto de Información Documentada propuesto por la Oficina de Integridad y Lucha contra la Corrupción, se ajusta a los lineamientos dispuestos en la Guía de Procedimientos GP-001-OPPM/UMO/001, denominada “Información Documentada del RENIEC”, primera versión, aprobada con Resolución Secretarial N° 000109-2024/SGEN/RENIEC (19SET2024), que establece en el numeral 6.1.b, entre los tipos de Información Documentada del RENIEC al Manual del Sistema de Gestión Integral de Riesgos; y, atendiendo a lo solicitado por la Oficina de Integridad y Lucha contra la Corrupción, ve por conveniente codificar la misma como Manual MGIR-001-OILCC/001 “Gestión Integral del Riesgo”, Primera Versión;

Que, asimismo, la Unidad de Modernización Organizacional de la Oficina de Planeamiento, Presupuesto y Modernización, señala que previo a la aprobación de la Información Documentada Manual MGIR-001-OILCC/001 "Gestión Integral del Riesgo", Primera Versión; es necesario dejar sin efecto:

*El Manual MGIR-200-GG/OFCR/001 "Manual Gestión Integral del Riesgo", segunda versión; aprobado mediante Resolución Secretarial N° 000029-2020/SGEN/RENIEC (04JUN2020), de conformidad con el numeral 6.2.c y demás pertinentes de la Guía de Procedimientos GP-001-OPPM/UMO/001, denominada "Información Documentada del RENIEC", primera versión, aprobada con Resolución Secretarial N° 000109-2024/SGEN/RENIEC (19SET2024);

*La Directiva DI 010-OIR/002 "Gestión Integral del Riesgo", primera versión, aprobada mediante Resolución Secretarial N° 000004-2023/SGEN/RENIEC (09ENE2023); de conformidad con el numeral 7.6 de la Directiva DI-001-OPPM/001 "Documentos Normativos del RENIEC", primera versión, aprobada por la Resolución Secretarial N° 000084-2024/SGEN/RENIEC (08JUL2024);

Que la Oficina de Asesoría Jurídica, mediante el documento de vistos emite opinión favorable sobre dejar sin efecto el Manual MGIR-200-GG/OFCR/001 "Manual Gestión Integral del Riesgo", segunda versión; aprobado mediante Resolución Secretarial N° 000029-2020/SGEN/RENIEC (04JUN2020) y la Directiva DI 010-OIR/002 "Gestión Integral del Riesgo", primera versión, aprobada mediante Resolución Secretarial N° 000004-2023/SGEN/RENIEC (09ENE2023); y, asimismo aprobar el Manual MGIR-001-OILCC/001 "Gestión Integral del Riesgo", Primera Versión;

Estando a lo informado por la Oficina de Planeamiento, Presupuesto y Modernización y a lo opinado por la Oficina de Asesoría Jurídica y, conforme con el Reglamento de Organización y Funciones del RENIEC, aprobado por Resolución Jefatural N° 000061-2024/JNAC/RENIEC (08ABR2024);

SE RESUELVE:

ARTÍCULO PRIMERO.- Dejar sin efecto:

1) El Manual MGIR-200-GG/OFCR/001 "Manual Gestión Integral del Riesgo", segunda versión; aprobado mediante Resolución Secretarial N° 000029-2020/SGEN/RENIEC (04JUN2020).

2) La Directiva DI 010-OIR/002 "Gestión Integral del Riesgo", primera versión, aprobada mediante Resolución Secretarial N° 000004-2023/SGEN/RENIEC (09ENE2023).

ARTÍCULO SEGUNDO.- Aprobar el Manual MGIR-001-OILCC/001 "Gestión Integral del Riesgo", Primera Versión, que como anexo forma parte integrante de la presente Resolución Secretarial.

ARTÍCULO TERCERO.- Encargar a la Oficina de Planeamiento, Presupuesto y Modernización la difusión del contenido de la presente Resolución Secretarial.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

GABRIELA BERTHA HERRERA TAN
Secretaria General
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

(GHT/rae)

MANUAL

GESTIÓN INTEGRAL DEL RIESGO

MGIR-001-OILCC/001

PRIMERA VERSIÓN

OFICINA DE INTEGRIDAD Y LUCHA CONTRA LA CORRUPCIÓN

ÍNDICE

I. OBJETO Y CAMPO DE APLICACIÓN

La Gestión Integral del Riesgo en el RENIEC, es el proceso sistemático, continuo y transversal que permite identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos institucionales, las disposiciones legales y normativas del Estado, especialmente aquellos vinculados con la integridad pública, la seguridad de la información, la calidad del servicio y la confianza ciudadana.

Este enfoque busca anticiparse a posibles eventos que puedan comprometer la transparencia, la eficiencia y eficacia en el otorgamiento de productos y prestación de servicios.

Su aplicación permite integrar otros sistemas de gestión reconocidos, como el de gestión de la calidad ISO 9001, seguridad de la información ISO 27001, sistema de gestión antisoborno ISO 37001, o cualquier otro sistema de gestión basado en el ciclo de mejora continua.

El presente manual es administrado por la Oficina de Integridad y Lucha Contra la Corrupción (OILCC); siendo de aplicación obligatoria por todos los Órganos del Registro Nacional de Identificación y Estado Civil en adelante RENIEC.

II. REFERENCIAS NORMATIVAS

2.1 **Ley N° 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 12 de julio de 1995 y sus modificatorias.

2.2 **Ley N° 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y su modificatoria.

2.3 **Ley N° 27658**, Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y sus modificatorias.

2.4 **Ley N° 27815**, Ley del Código de Ética de la Función Pública, del 13 de agosto de 2002 y sus modificatorias.

2.5 **Ley N° 28716**, Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.

2.6 **Ley N° 29733**, Ley de Protección de Datos Personales, del 3 de julio de 2011 y sus modificatorias.

2.7 **Ley N° 27806**, aprueba Ley de Transparencia y Acceso a la Información Pública, del 2 de agosto de 2002 y sus modificatorias.

2.8 **Decreto Legislativo N° 1370**, Decreto Legislativo que modifica la Ley N° 27269, Ley de Firmas y Certificados Digitales y el Decreto Ley N° 25632, Ley Marco de comprobantes de pago, del 2 de agosto de 2018.

2.9 **Decreto Legislativo N° 1412**, Decreto Legislativo que aprueba la Ley de Gobierno Digital, del 13 de setiembre de 2018.

2.10 **Decreto Supremo N.º 015-98-PCM**, que aprueba el Reglamento de Inscripciones del Registro Nacional de Identificación y Estado Civil, del 25 de abril de 1998 y sus modificatorias.

2.11 **Decreto Supremo N.º 030-2002-PCM**, que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado, del 3 de mayo de 2002.

2.12 **Decreto Supremo N° 052-2008-PCM**, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, del 19 de julio de 2008 y sus modificatorias.

2.13 **Decreto Supremo N° 004-2013-PCM**, que aprueba la Política Nacional de Modernización de la Gestión Pública, del 9 de enero de 2013.

2.14 **Decreto Supremo N° 092-2017-PCM**, que aprueba la Política Nacional de Integridad y Lucha Contra la Corrupción, del 14 de setiembre de 2017.

2.15 **Decreto Supremo N° 042-2018-PCM**, Decreto Supremo que establece medidas para Fortalecer la Integridad Pública y Lucha Contra la Corrupción, del 22 de abril de 2018.

2.16 **Decreto Supremo N° 004-2019-JUS**, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, del 25 de enero de 2019 y sus modificatorias.

2.17 **Decreto Supremo N° 021-2019-JUS**, Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 11 de diciembre de 2019 y su modificatoria.

2.18 **Decreto Supremo N° 029-2021-PCM**, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, del 19 de febrero de 2021 y su modificatoria.

2.19 **Decreto Supremo N° 021-2019-JUS**, aprueba el Texto Único Ordenado de la Ley 27806 Ley de Transparencia y Acceso a la Información Pública, del 11 de diciembre de 2019 y su modificatoria.

2.20 **Decreto Supremo N° 103-2022-PCM**, que aprueba la “Política Nacional de Modernización de la Gestión Pública al 2030”, del 21 de agosto de 2022.

2.21 **Decreto Supremo N° 148-2024-PCM**, Decreto Supremo que aprueba el Modelo de Integridad para fortalecer la capacidad de prevención y respuesta frente a la corrupción en las entidades del sector público, del 28 de diciembre de 2024.

2.22 **Resolución de Secretaría de Integridad Pública N° 001-2019-PCM/SIP**, que aprueba la Directiva N° 001-2019-PCM/SIP “Lineamientos para la Implementación de la Función integridad en las Entidades de la Administración Pública”, del 24 de julio de 2019.

2.23 **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", del 28 de junio de 2021.

2.24 **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", del 5 de enero 2023.

2.25 **Resolución de Secretaría de Integridad Pública N° 001-2024-PCM/SIP**, que aprueba la "Directiva para la incorporación y ejercicio de la función de integridad en las entidades de la administración pública", del 2 de marzo de 2024.

2.26 **Resolución de Secretaría de Gestión Pública N° 002-2025-PCM-SGP**, que aprueba la Norma Técnica N° 002-2025-PCM/SGP, Norma Técnica para la Gestión por Procesos en las entidades de la Administración Pública, del 23 de febrero de 2025.

2.27 **Resolución de Contraloría Nº 320-2006-CG**, Aprueban las Normas de Control Interno, del 3 de noviembre de 2006.

2.28 **Resolución de Contraloría Nº 146-2019-CG**, Aprueban la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del Estado", del 17 de mayo de 2019 y sus modificatorias.

2.29 **Resolución Jefatural N° 162-2022/JNAC/RENIEC**, aprobar la actualización de la Política y Objetivos de la Gestión Integral del Riesgo del RENIEC, del 26 de setiembre de 2022.

2.30 **Resolución Jefatural Nº 061-2024/JNAC/RENIEC**, aprobar el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 8 de abril de 2024 y modificatoria.

2.31 **Resolución Jefatural N° 033-2025/JNAC/RENIEC**, designar a la Jefa de la Oficina de Integridad y Lucha Contra la Corrupción la función de cumplimiento antisoborno del Registro Nacional de Identificación y Estado Civil, del 19 de febrero de 2025.

2.32 **Resolución Jefatural N° 045-2025/JNAC/RENIEC**, aprobar el Plan Estratégico Institucional correspondiente al periodo 2025-2030 del RENIEC, del 1 de marzo de 2025.

2.33 **Resolución Secretarial N° 115-2022/SGEN/RENIEC**, aprobar la Directiva DI-003-SGEN/001 "Gestión Documental del RENIEC", del 7 de octubre de 2022.

2.34 **Resolución Secretarial Nº 084-2024/SGEN/RENIEC**, aprobar la Directiva DI-001-OPPM/001 "Documentos normativos del RENIEC", del 8 de julio de 2024.

2.35 **Resolución Secretarial Nº 109-2024/SGEN/RENIEC**, aprobar la Guía de Procedimientos GP-001-OPPM/001 "Información Documentada del RENIEC", Primera Versión, del 19 de setiembre de 2024.

2.36 **Resolución Secretarial N° 177-2025/SGEN/RENIEC**, que aprueba el Mapa de Proceso Nivel 0 y 1 del RENIEC, del 14 de noviembre de 2025.

2.37 **Resolución Directoral N° 014-2018-INACAL/DN**, aprueban Normas Técnicas Peruanas, especificación Técnica Peruana y Reporte Técnico Peruano, entre las que se encuentra la NTP-ISO 31000:2018 Gestión del Riesgo. Directrices, 2ª Edición; del 04 de julio de 2018.

2.38 **Resolución Directoral N° 022-2022-INACAL/DN**, aprueban Normas Técnicas Peruanas entre las que se encuentra la NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la seguridad, Sistemas de gestión de la seguridad de la información. Requisitos, 3° Edición; del 12 de enero de 2023.

2.39 **Resolución Directoral N° 022-2022-INACAL/DN**, aprueban Normas Técnicas Peruanas entre las que se encuentra la NTP-ISO/IEC 27002:2022 Seguridad de la Información, ciberseguridad y protección de la seguridad, Controles de seguridad de la información. 2° Edición, del 12 de enero de 2023.

2.40 **Resolución Directoral N° 000017-2025-INACAL/DN**, Aprueban Normas Técnicas Peruanas sobre sistemas de gestión antisoborno, entre las que se encuentra la NTP-ISO 37001:2025 Sistemas de Gestión Antisoborno, Requisitos con orientación para su uso. 2° Edición, del 7 de agosto de 2025.

III. TÉRMINOS Y DEFINICIONES

3.1 SIGLAS

En el presente Manual se utilizan las siguientes siglas:

Tabla N° 1: Siglas de las unidades de organización del RENIEC

SIGLAS DE LAS UNIDADES DE ORGANIZACIÓN DEL RENIEC	
RENIEC	Registro Nacional de Identificación y Estado Civil
DCSD	Dirección de Certificación Servicios Digitales
DRC	Dirección de Registros Civiles
DRE	Dirección de Registro Electoral
DRI	Dirección de Registros de Identificación
DSR	Dirección de Servicios Registrales
GG	Gerencia General
GIR	Gestión Integral del Riesgo
JNAC	Jefatura Nacional
OAF	Oficina de Administración y Finanzas
OAJ	Oficina de Asesoría Jurídica
OFCI	Oficina de Formación Ciudadana e Identidad
OILCC	Oficina de Integridad y Lucha contra la Corrupción
OPH	Oficina de Potencial Humano
OPPM	Oficina de Planeamiento, Presupuesto y Modernización
OSCD	Oficial de Seguridad y Confianza Digital

OSDN	Oficina de Seguridad y Defensa Nacional
OTI	Oficina de Tecnologías de la Información
SGEN	Secretaria General
UGTI	Unidad de Gobierno de Tecnologías de la Información
Referencia: Cuadro de Equivalencias y Siglas de los órganos y unidades orgánicas del RENIEC Resolución Jefatural N° 000067-2024/JNAC/RENIEC, de fecha 22 de abril del 2024.	

Tabla N° 2: Siglas utilizadas en la Gestión Integral del Riesgo

SIGLAS UTILIZADAS EN LA GESTION INTEGRAL DEL RIESGO	
SGSI	Sistema de Gestión de la Seguridad de la Información
SITD	Sistema Integrado de Trámite Documentario
PAA	Plan de Acción Anual
PAAMC	Plan de Acción Anual Medidas de Control
PAAMR	Plan de Acción Anual Medidas de Remediación
PEI	Plan Estratégico Institucional
PGIR	Plan de Gestión Integral del Riesgo
PGO	Plan de Gestión de Oportunidades

Tabla N° 3: Cuadro de siglas al exterior de la Entidad

SIGLA	DESCRIPCIÓN
CGR	Contraloría General de la Republica
COSO	Committee of Sponsoring Organizations of the Treadway Commission (Comité de Organizaciones Patrocinadoras de la Comisión Treadway)
ISO	International Organization for Standardization (Organización Internacional de Estandarización)
NTP	Norma Técnica Peruana
PCM	Presidencia del Consejo de Ministros
SCI	Sistema de Control Interno
SIP	Secretaria de Integridad Publica

FUENTE: Elaboración OILCC

3.2 DEFINICIONES

3.2.1 Activo de Información

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.

3.2.2 Acto de Corrupción

Comprenden 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, que contiene también las sanciones aplicables en cada caso. Aquellos de mayor recurrencia son el peculado, la colusión, la negociación incompatible y el cohecho (o soborno).

Los actos de corrupción implican una grave vulneración de valores, principios y normas que regulan el correcto y regular funcionamiento de la administración pública. (Guía para la Gestión de Riesgos que afectan la Integridad Pública).

3.2.3 Amenaza

Potencial ocurrencia de un hecho que pueda afectar el logro de los objetivos institucionales.

Para seguridad de la Información es la causa potencial de un incidente no deseado, el cual puede causar el daño a uno o varios activos de información.

3.2.4 Atributos

Característica del producto que impacta de manera directa en la atención de las necesidades y expectativas de las personas. Pueden ser atributos de calidad que impactan en la satisfacción de las personas; o atributos establecidos por los entes rectores para la solución de un problema público. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.5 Confidencialidad

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

3.2.6 Contexto Externo

Es el conjunto de elementos o circunstancias externas que influyen o condicionan los acontecimientos o hechos, sin los cuales no se podría comprender correctamente el entorno de la organización.

3.2.7 Contexto Interno

Es el conjunto de elementos o circunstancias internas que influyen o condicionan los acontecimientos o hechos, sin los cuales no se podría comprender correctamente el entorno de la organización.

3.2.8 Control

Medida que mantiene y/o modifica un riesgo. Un control contribuye a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente. Se constituye en el mecanismo por el cual la Entidad logre comprobar que las

cosas se realicen como fueron previstas para garantizar el cumplimiento de los objetivos. Medidas de protección desplegadas para controlar un riesgo.

3.2.9 Control existente/implementado

Medida existente/implementada para modificar el riesgo en la etapa de Análisis y Valoración, así como en el Tratamiento del riesgo.

3.2.10 Corrupción

Acción u omisión que determina el mal uso del poder público o privado para obtener un beneficio indebido: económico, no económico o ventaja directa o indirecta; por agentes públicos, privados o ciudadanos; vulnerando principios y deberes éticos, normas y derechos fundamentales. (Guía para la Gestión de Riesgos que afectan la Integridad Pública)

3.2.11 Criterios del Riesgo

Son los términos de referencia respecto a los que se evalúa la importancia de un riesgo. Se basan en los objetivos de la Entidad, en el contexto externo e interno, normas, leyes, políticas, buenas prácticas y otros requisitos que se deben cumplir.

3.2.12 Disponibilidad

Propiedad de la información de estar disponible y utilizable cuando lo requiera una Entidad autorizada.

3.2.13 Dueño del Proceso

Persona que ocupa el cargo y tiene la responsabilidad del manejo de la unidad de organización que ejecuta un proceso y garantiza que su producto sea ofrecido según las necesidades y expectativas de las personas. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.14 Efectividad

La capacidad de un proceso de gestión de riesgos para lograr su objetivo principal mitigar o eliminar los riesgos de manera eficiente y efectiva, minimizando el impacto negativo en la Entidad

3.2.15 Evento

Ocurrencia o cambio de un conjunto particular de circunstancias

3.2.16 Evento de pérdida

Es la materialización de un riesgo que genera una o varias pérdidas.

3.2.17 Fuente de Riesgo

Elemento que, por sí solo o en combinación con otros, presenta el potencial de generar un riesgo.

3.2.18 Gestión Integral del Riesgo

Es la aplicación sistemática de políticas, procedimientos y prácticas de gestión que brindan una seguridad razonable para el cumplimiento de los objetivos estratégicos institucionales. Se implanta como un sistema de gestión que constituye una herramienta para la toma de decisiones y que permite integrar otros sistemas de gestión reconocidos, como el de gestión de la calidad ISO 9001, seguridad de la información ISO 27001, sistema de gestión antisoborno ISO 37001, o cualquier otro sistema de gestión basado en el ciclo de mejora continua.

3.2.19 Gestión por procesos

Forma de planificar, organizar, dirigir y controlar las actividades de trabajo con un enfoque sistémico y transversal, para lograr que las diferentes unidades de organización actúen como un ente unificado, para contribuir con el propósito de satisfacer las necesidades y expectativas de las personas y crear valor público. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.20 Inconducta Funcional

La inconducta funcional es un comportamiento indebido, por acción u omisión, que implica el incumplimiento de una función – la transgresión de los deberes y las prohibiciones – derivada de la contravención del ordenamiento jurídico administrativo y las normas internas de la entidad. Para ser considerada como tal, la inconducta funcional debe estar tipificada con disposiciones claramente establecidas y debe tener una sanción definida. (Guía para la Gestión de Riesgos que afectan la Integridad Pública)

3.2.21 Impacto o Consecuencias

Resultado de un evento o incidente. El impacto puede ser positivo (oportunidad) o negativo sobre los objetivos estratégicos institucionales. En el caso de los riesgos de Seguridad de la Información es el daño sobre el activo derivado de la materialización de la amenaza.

3.2.22 Incidente de Seguridad de Información

Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones y amenazar la seguridad de la información de la entidad pública

3.2.23 Incidente de Seguridad Digital

Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

3.2.24 Integridad (Seguridad de la información)

Propiedad de la información de integridad.

3.2.25 Medida de Control

Son las actividades de supervisión de las acciones establecidas para reducir el nivel de exposición de los riesgos que pasaron a la etapa de tratamiento. Se enfocan en prevenir o controlar los riesgos potenciales y, en esencia, son la fase de acción dentro del ciclo de gestión de riesgos. (Directiva 006-2019-CG/INTEG Contraloría General de la Republica)

3.2.26 Medio de verificación

Documento que evidencia o sustenta la implementación de la medida de control y/o acción.

3.2.27 Nivel de proceso

Es la clasificación de los procesos de acuerdo a su desagregación. El nivel 0, también llamado Macroproceso, es el nivel más agregado. Luego se va desagregando en nivel 1, nivel 2 hasta el último nivel n. (Norma Técnica N° 002 -2025-PCM-SGP).

3.2.28 Oportunidad

Una oportunidad se define como una situación o circunstancia externa o interna que, si se aprovecha, puede generar un beneficio o ventaja para la organización, contribuyendo a la consecución de sus objetivos.

3.2.29 Plan de Acción de Anual Medidas de Control (PAAMC)

Documento de gestión que detalla las medidas de control, acciones, plazos, responsables y medios de verificación que la entidad elabora y ejecuta para mitigar los riesgos identificados en los productos o servicios priorizados que brinda a los ciudadanos y cuyo resultado es reportado a la Contraloría General de la Republica en el marco de la implementación del Sistema de Control Interno.

3.2.30 Plan de Gestión Integral del Riesgo (PGIR)

Documento de gestión interno que detalla las medidas de control, acciones, plazos, responsables y medios de verificación que la entidad elabora y ejecuta para mitigar los riesgos identificados en los productos o servicios no priorizados que brinda a los ciudadanos y cuyo resultado es reportado a la Alta Dirección.

3.2.31 Política de la Gestión Integral del Riesgo

Es la línea de acción para la implementación, sostenibilidad y mejora continua de la Gestión del Riesgo en el Registro Nacional de Identificación y Estado Civil y es aprobada por la Jefatura Nacional.

3.2.32 Probabilidad

Posibilidad que suceda un determinado evento, puede medirse objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos.

3.2.33 Proceso

Conjunto de actividades mutuamente relacionadas que interactúan y que agregan valor, las cuales transforman elementos de entrada en productos. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.34 Procesos de apoyo o de soporte

Son aquellos que proporcionan los recursos para elaborar los productos previstos por la entidad. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.35 Procesos estratégicos

Son aquellos que definen las políticas, el planeamiento institucional, las estrategias, los objetivos y metas de la entidad, que aseguran la provisión de los recursos necesarios para su cumplimiento, así como aquellos destinados al seguimiento, evaluación y mejora de la entidad. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.36 Procesos misionales u operativos

Son aquellos que se encargan de elaborar los productos (bienes, servicios o regulaciones) previstos por la entidad, por lo que tienen una relación directa con las personas que los reciben. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.37 Producto

Son los bienes, servicios o regulaciones, resultante de un proceso y que es entregado a las personas, a una entidad o a una unidad de organización de la entidad, con el propósito de implementar los objetivos de política pública y crear valor público. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.38 Producto Priorizado

Es el bien o servicio que ha sido priorizado con la finalidad de identificar los riesgos que puedan afectar su provisión, tomando en cuenta discrecionalmente entre otros, uno o varios de los siguientes criterios: Relevancia para la población; Presupuesto asignado al producto; Contribución al logro del Objetivo Estratégico Institucional de Tipo I (PEI) o Resultado Específico (Programa Presupuestal) e Indicadores de desempeño de productos o servicios que se otorgan a la población demandante de éstos, de acuerdo a sus indicadores establecidos en el PEI.

3.2.39 Proceso Gestión Integral del Riesgo

Comprende la realización de actividades necesarias para el tratamiento de los riesgos o aprovechamiento de oportunidades que se presentan en la Entidad. Estas actividades son la Planificación, Identificación, Análisis, Valoración, Tratamiento, Seguimiento y Revisión, Comunicación y Consulta, Registro e Informe.

3.2.40 Riesgo

Es la posibilidad de ocurrencia de un evento adverso o positivo, respecto al cumplimiento de los objetivos estratégicos institucionales.

Posibilidad de que ocurra un evento adverso que afecte el logro del objetivo del proceso. (Norma Técnica N° 002 -2025-PCM-SGP)

Efecto de la incertidumbre sobre la consecución de los objetivos. (ISO NTP 31000:2018).

3.2.41 Riesgo Aceptado

Es el riesgo que acepta la Entidad. Decisión de que puede tolerarse el riesgo considerando su nivel de exposición.

3.2.42 Riesgo Inherente

Es aquel que está intrínsecamente ligado a una actividad, proceso o sistema antes de que se implementen medidas de control o gestión de riesgos.

3.2.43 Riesgo Residual

Es el riesgo remanente después de implementar las medidas de control en la etapa de tratamiento al riesgo.

3.2.44 Servicios

Son los productos intangibles que responden a las necesidades de las personas y que son entregados por las entidades públicas, en cumplimiento de sus funciones. (Norma Técnica N° 002 -2025-PCM-SGP)

3.2.45 Sistema de Gestión Antisoborno

Conjunto de políticas, procedimientos y controles, basado en la norma internacional ISO 37001, que ayuda a una organización a prevenir, detectar y responder ante los actos de soborno. Su objetivo es fomentar una cultura de integridad y transparencia, reducir los riesgos de corrupción, cumplir con las leyes y mejorar la reputación.

3.2.46 Sistema de Gestión de la Calidad

Es un conjunto de políticas, procesos y procedimientos que una organización implementa para asegurar que sus productos y servicios cumplen consistentemente los requisitos del cliente y las regulaciones aplicables, al mismo tiempo que promueve la mejora continua

3.2.47 Sistema de Gestión de Seguridad de la Información

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y

aplicar controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI; y consta de políticas, procedimientos, directrices, recursos y actividades asociados, gestionados colectivamente por una organización, en la búsqueda de proteger sus activos de información.

3.2.48 Tolerancia

Es el nivel de exposición al riesgo que "acepta" la Entidad, el cual no requiere la adopción de medidas adicionales, solamente realizar un monitoreo constante para prevenir que el riesgo pueda incrementar su nivel de exposición. En la Entidad el nivel de riesgo tolerado es "Bajo".

3.2.49 Valor público

Es el fin que persigue la gestión por procesos y que se crea cuando los productos que generan las entidades públicas atienden las necesidades y expectativas de las personas y optimizan su gestión interna, generando beneficios a la sociedad, y, cuando se optimiza la gestión interna a través del uso más eficiente de los recursos públicos.

3.2.50 Vulnerabilidad (riesgo de seguridad de la información)

Debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los ciberdelincuentes para comprometer la confidencialidad, integridad y disponibilidad. Ausencia o debilidad de un control que puede ser explotado por una o más amenazas.

IV. RESPONSABLES

Para la aplicación, implementación y mejora continua de la gestión del riesgo en la entidad se han definido los siguientes roles y responsabilidades:

4.1 De la Jefatura Nacional (JNAC)

Es la máxima autoridad jerárquica en la entidad, responsable de la implementación de la Gestión Integral del Riesgo, se encarga de:

a) Aprobar la propuesta de productos priorizados incluidos en el Plan Gestión Integral del Riesgo (PGIR) y el Plan de Acción Anual – Medidas de Control (PAAMC)
b) Aprobar la política y objetivos de la Gestión Integral del Riesgo en la Entidad.
c) Aprobar los entregables del Sistema de Control Interno a través del aplicativo informático de la CGR.

4.2 De la Secretaría General (SGEN)

Es la máxima autoridad administrativa en la Entidad, responsable de supervisar la implementación de la Gestión Integral del Riesgo en los procesos de soporte y estratégicos, de corresponder, tiene a su cargo las siguientes funciones:

a) Coordinar y articular con la OILCC para garantizar la implementación de la Gestión Integral del Riesgo en la Entidad.
b) Disponer a los órganos a su cargo la implementación de la Gestión Integral del Riesgo en sus procesos.
c) Visar y gestionar con la JNAC la aprobación del Plan de Acción Anual Medidas de Control (PAAMC)
d) Difundir a los órganos de la Entidad, los planes de Gestión Integral del Riesgo (PGIR y PAAMC), así como también el Plan de Gestión de Oportunidades (PGO) y disponer su ejecución dentro de los plazos establecidos.

4.3 De la Gerencia General (GG)

Es la máxima autoridad ejecutiva en la Entidad, responsable de supervisar la implementación de la Gestión Integral del Riesgo en los procesos misionales, tiene a su cargo las siguientes funciones:

a) Coordinar y articular con la OILCC para garantizar la implementación de la Gestión Integral del Riesgo en la Entidad.
b) Disponer a los órganos a su cargo la implementación de la Gestión Integral del Riesgo en sus procesos.
c) Aprobar y difundir a los órganos a su cargo, los planes de Gestión Integral del Riesgo (PGIR y PAAMC) y el Plan de Gestión de Oportunidades (PGO) y disponer su ejecución dentro de los plazos establecidos.

4.4 De la Oficina de Integridad y Lucha Contra la Corrupción (OILCC)

Es el órgano responsable de la Gestión Integral del Riesgo en la entidad, integrando las diferentes normativas vinculadas en la materia (Contraloría General de la República, Secretaría de Integridad Pública y otros que puedan corresponder), tiene a su cargo las siguientes funciones:

a) Formular y actualizar el marco normativo que regulan la Gestión Integral del Riesgo (GIR) en la Entidad.
b) Promover la cultura de gestión integral del riesgo en la entidad.
c) Establecer las pautas para el PGIR/PAAMC/PGO, que incluye: difusión del plan de trabajo, plazos para el reporte periódico, formatos de trabajo, entre otros.
d) Dirigir la implementación de la Gestión de Riesgos que afecta la integridad pública.
e) Gestionar en conjunto con el Oficial de la Calidad, Oficial de Seguridad y Confianza Digital y el responsable de la función Cumplimiento/Antisoborno, la identificación, análisis, valoración y tratamiento de los riesgos en los productos priorizados y no priorizados de la Entidad a cargo de los órganos responsables.
f) Solicitar a los órganos y unidades orgánicas la designación de los gestores lideres y equipos de riesgos/gestores operativos; así como actualizar el registro según corresponda.
g) Capacitar a gestores lideres y equipos de riesgos/gestores operativos de los órganos de la entidad.
h) Supervisar la implementación de los planes de Gestión Integral del Riesgo; así como validar la efectividad de las medidas de control implementadas.
i) Consolidar y generar reportes sobre los PGIR/PAAMC aprobados en la entidad.
j) Informar del resultado mensual del avance del PGIR/PAAMC a la alta dirección

k) Gestionar la evaluación semestral y anual del Sistema de Control Interno (eje gestión de riesgos), reportando los avances y resultados a través del aplicativo SCI de la Contraloría General de la Republica.
l) Realizar el seguimiento y revisión mensual de los PGIR/PAAMC/PGO, remitido por los oficiales y los órganos responsables (riesgos que afectan la integridad pública).
m) Comunicar a los órganos la retroalimentación mensual del PGIR/PAAMC/PGO.
n) Brindar asistencia técnica a los dueños de los procesos y gestores lideres de riesgos en la Identificación, análisis, valoración y tratamiento de las oportunidades (Plan de Gestión de Oportunidades – PGO), identificadas en sus procesos.
o) Revisar y consolidar las respuestas del cuestionario Evaluación del SCI según las fichas de la CGR relacionadas al eje gestión de riesgos (semestral y anual)

4.5 Del Oficial de la Calidad, Oficial de Seguridad y Confianza Digital y Responsable de la función de Cumplimiento/Antisoborno.

Se encargan de brindar el asesoramiento y asistencia técnica a los órganos en el proceso de la gestión integral del riesgo, así como absolver las consultas relacionadas en el marco de su competencia, se encargan de:

a) Coordinar con los dueños de los procesos y gestores lideres de riesgos las acciones que correspondan en el marco de su competencia.
b) Revisar y validar la efectividad de cada medida de control
c) Evaluar la pertinencia y factibilidad de las medidas de control definidas en los planes de gestión integral del riesgo.
d) Supervisar la implementación de los planes PGIR/PAAMC y validar la efectividad de las medidas de control implementadas, relacionadas a los riesgos de tipo operativo (Oficial de la Calidad), seguridad de la información (Oficial de Seguridad y Confianza Digital) y riesgos que afectan la integridad pública (responsable de la función de Cumplimiento/Antisoborno).
e) Realizar la revisión y retroalimentación para la elaboración y el seguimiento del PGIR/PAAMC en coordinación con el proceso y la OILCC.
f) Remitir los resultados de la evaluación de los planes del PGIR/PAAMC a la OILCC, para su consolidación y presentación a la alta dirección.
g) Participar en conjunto con el equipo de la OILCC en la capacitación que se realiza a los gestores lideres, equipos de riesgos/gestores operativos.
h) Brindar asistencia técnica a los dueños de los procesos y gestores lideres de riesgos en la Identificación, análisis, valoración y tratamiento de las oportunidades (Plan de Gestión de oportunidades – PGO), identificadas en sus procesos.
i) Supervisar la implementación de los planes PGO y validar la efectividad de las acciones implementadas, relacionadas a las oportunidades de tipo operativo (Oficial de la Calidad), seguridad de la información (Oficial de Seguridad y Confianza Digital) e integridad pública (responsable de la función de Cumplimiento/Antisoborno)

4.6 De la Oficina de Planeamiento, Presupuesto y Modernización

Es el órgano responsable de gestionar la implementación del modelo de gestión por procesos, así como elaborar el mapa de procesos institucional, el presupuesto operacional y realizar la identificación de los productos y servicios en la entidad, tiene a su cargo las siguientes funciones:

a) Elaborar y actualizar el mapa de procesos institucional, fuente de información importante e imprescindible para la identificación de riesgos en la Entidad.
b) Identificar los productos, relacionado con el mapa de procesos institucional (procesos misionales, de soporte, estratégicos, desde el nivel 0 en adelante, con sus respectivos códigos, identificando al órgano dueño de proceso).
c) Formular el diagnóstico situacional respecto al diseño y funcionamiento de sus procesos que permiten la entrega de productos y servicios a la población (contexto interno), así como evaluar lo relacionado de escenarios contextuales a nivel nacional (contexto externo); información que servirá como insumo para la identificación de riesgos y oportunidades en los procesos de la entidad, para ello se coordina con todos los órganos de la entidad.
d) Identificar las características y condiciones como atributos de calidad que tienen los productos y servicios que entrega la Entidad.
e) Prever el presupuesto operacional para los productos priorizados de acuerdo con el modelo establecido por la CGR.
f) Proponer a la Alta dirección los productos a priorizar en el Reniec y que serán incorporados en la gestión de riesgos, incluidos en el PGIR y PAAMC.

4.7 De los Órganos de la Entidad designados como dueños de los procesos

Son los órganos responsables de organizar y dirigir la gestión integral del riesgo en coordinación con la OILCC y con los oficiales de los sistemas de gestión, sobre la disponibilidad de recursos para la implementación de los planes y coordina con los órganos y unidades orgánicas que participan en la gestión integral del riesgo en los procesos a su cargo, se encarga de:

a) Designar o ratificar a los Coordinadores de Integridad, Control Interno, Gestores Líderes y Equipos de riesgos, titulares y suplentes. Asimismo, reportan de manera permanente a la OILCC cuando se produzca algún cambio; a fin de mantener el registro actualizado el mismo que constituye una fuente de información importante para realizar labores de difusión, capacitación y reconocimiento.
b) Designar o ratificar al funcionario del órgano responsable quien participara junto con el equipo de riesgos durante el proceso de identificación, análisis, valoración y tratamiento de los riesgos.
c) Identificar:
   - Los pasos o actividades del proceso, así como los atributos y oportunidades.
   - Los riesgos inherentes, así como los controles existentes en el proceso, para la identificación y valoración del riesgo residual.
   - Las causas y efectos o consecuencias de los riesgos, para valorar la probabilidad e impacto para obtener el nivel de exposición al riesgo.

d) Dirigir la reevaluación de riesgos, la identificación, análisis, valoración y tratamiento que corresponden.
e) Documentar la participación del funcionario y servidores integrantes del equipo de riesgos mediante (actas, informes, tomas fotográficas u otros), así como uso de las herramientas de recolección de información (análisis de causa efecto, Ishikawa, cinco porque, lluvia de ideas, análisis de diagrama de procesos, entrevistas, encuestas, registro de incidentes, etc.) en todas las etapas del proceso de gestión de riesgos (identificación, análisis, valoración y tratamiento de los riesgos).
f) Proponer medidas de control y acciones que sean factibles de implementar por la entidad, con la finalidad de mitigar y/o reducir el nivel de exposición del riesgo identificado; estas medidas deben incluir la identificación de responsables, plazos y medios de verificación.
g) Revisar, aprobar y remitir el PGIR, PAAMC y PGO del proceso a su cargo.
h) Reportar de manera mensual las evidencias del avance en la ejecución del PGIR, PAAMC y PGO.
i) Remitir al OILCC la información, que sustenten las respuestas del cuestionario Evaluación del SCI según las fichas de la CGR del eje gestión de riesgos (semestral y anual)

4.8 Del Gestor Líder de Riesgos

Responsable designado por el Órgano correspondiente, quien realizará las coordinaciones con los Oficiales y la OILCC encargados de la Gestión Integral del Riesgo. Se encarga de:

a) Coordinar:
   - Con el dueño del proceso las actividades de la gestión integral del riesgo para su revisión y aprobación.
   - Con el equipo de riesgos/gestores operativos la implementación de la Gestión Integral del Riesgo.
   - Con la OILCC, Oficial de Calidad, Oficial de Seguridad y Confianza Digital y Responsable de la función de Cumplimiento/Antisoborno las acciones correspondientes a la Gestión Integral del Riesgo.
   - Con los órganos involucrados en su proceso, las acciones correspondientes a la gestión integral del riesgo.

b) Participar:
   - En la Gestión Integral del Riesgo identificando los controles existentes para la gestión de riesgos operativos, que afectan la integridad pública y de seguridad de la información.
   - En la identificación, análisis, valoración y tratamiento del PGIR, PAAMC y PGO, revisando y validando el análisis de la identificación de los riesgos en el proceso, la valoración de los riesgos identificados y su tratamiento.
   - En el seguimiento del PGIR/PAAMC, reportando el estado de la implementación de su proceso.
   - En la reevaluación de riesgos, evaluando la efectividad de la medida de control, revisa el riesgo, valora y propone las nuevas medidas de control.

4.9 Del Equipo de Riesgos o Gestores Operativos

Grupo multifuncional conformado por el Gestor Líder de Riesgos y personal de los Órganos con conocimientos en procesos que gestiona los riesgos y reporta sus resultados. Es designado por el Dueño del Proceso y se encarga de las siguientes actividades:

a) Participar:
- En la identificación de riesgos de su proceso, identificando el producto, sus atributos y oportunidades, así como las actividades y tareas del proceso, comunicando al gestor líder los riesgos identificados, considerando el contexto interno y externo de la entidad, utilizando las herramientas para recolección de datos.
- En el análisis, valorando la probabilidad e impacto de la materialización del riesgo inherente, calcula el nivel de exposición del riesgo e identifica y evalúa los controles existentes.
- En la valoración del riesgo, considerando los controles existentes para calcular la probabilidad e impacto del riesgo residual. Además, selecciona la opción de tratamiento de acuerdo al nivel de tolerancia establecido por la Entidad
- En el seguimiento del PGIR/PAAMC, reportando el estado de la implementación de su proceso.
- En la reevaluación de riesgos, evaluando la efectividad de la medida de control, revisa el riesgo, valora y propone las nuevas medidas de control.
- En la valoración del riesgo, considerando los controles existentes para calcular la probabilidad e impacto del riesgo residual. Además, selecciona la opción de tratamiento de acuerdo al nivel de tolerancia establecido por la Entidad.
- En el tratamiento del riesgo e identifica el riesgo a tratar, establece la medida de control alineada a las causas y efectos, plazos de ejecución, medios de verificación y responsables. De igual forma, establece las acciones por cada medida de control, así como los plazos de ejecución, medios de verificación y órganos involucrados

b) Considerar durante la identificación de riesgos en sus procesos, posibles eventos que, de materializarse podrían:
- Afectar las condiciones y atributos del producto o servicio (oportunidad, cobertura, calidad, continuidad, del servicio, personal calificado, u otras).
- Generar actos de corrupción o inconducta funcional que pudieran afectar la integridad pública.
- Generar fraudes financieros o contables (registros contables y administrativos falsos), sobrecostos o transferencia de recursos para fines distintos al original.
- Afectar el cumplimiento de las funciones desarrolladas por los funcionarios y servidores al encontrarse influenciados, inducidos o presionados a efectuar conductas irregulares.

- Generar posible influencia de consultores o actores externos en las decisiones de los funcionarios para realizar requerimientos de bienes o servicios.
- Generar pagos tardíos (retrasados) a los proveedores.
- Generar el favorecimiento a un postor o postulante, dentro de un proceso de contratación, entre otros.

c) Reportar durante el seguimiento y reporte del estado de implementación de cada una de las acciones establecidas del PGIR, PAAMC y PGO, efectuando el seguimiento, considerando lo siguiente:

- Que los medios de verificación de las acciones guarden relación con la medida de control y con los documentos de sustento declarados. Asimismo, toda evidencia remitida deberá contar con firma digital o visto bueno del responsable de su formulación.
- En caso exista más de un medio de verificación, estos deben ser nombrados en orden cronológico o según su importancia (de mayor a menor). Asimismo, en caso sea posible serán unidos en un único archivo en formato PDF.
- Si la medida de control involucra a otro órgano de la Entidad, se deberá remitir el acta de reunión que evidencie la coordinación previa con dicho órgano.
- Durante la ejecución de las acciones y medidas de control contenidas en el PGIR, PAAMC y PGO se deberá describir, en la sección “seguimiento del proceso”, de acuerdo al mes correspondiente las gestiones realizadas que sustenten el cumplimiento del avance planificado.
- Si durante la ejecución de las acciones y medidas de control contenidas en el PGIR, PAAMC y PGO se identifica alguna problemática que pueda afectar el cumplimiento oportuno de estas medidas, se deberá registrar dicha información en la columna de “Problemática”, señalando las posibles alternativas de solución en la columna de “Recomendaciones de mejora”.

V. CONTENIDO

5.1 ASPECTOS TRANSVERSALES

5.1.1 PLANIFICACION

Es el proceso para establecer los objetivos e implementar todas las actividades de la Gestión Integral del Riesgo, siendo importante una planificación cuidadosa y explícita para mejorar las posibilidades de éxito de su aplicación en la Entidad.

5.1.1.1 ALCANCE DE LA GESTION INTEGRAL DEL RIESGO

El RENIEC ha definido su alcance en la Gestión Integral del Riesgo, considerando su aplicación en los procesos misionales, de soporte y estratégicos, en sus productos priorizado y no priorizado en alineamiento a los objetivos estratégicos de la Entidad, teniendo como base la gestión por procesos.

Este alcance es coherente con el desarrollo y ejecución de la Política de Gestión Integral del Riesgo alineada con sus objetivos estratégicos institucionales.

El desarrollo de un adecuado ambiente interno, para la Gestión Integral del Riesgo, es promovido por el Titular de la Entidad, la Alta Dirección y los Órganos de la Entidad, como parte esencial de la asignación de responsabilidades en las actividades para la Gestión Integral del Riesgo y la generación del pensamiento basado en riesgos como parte de la cultura de la Entidad. El compromiso por parte de los funcionarios y servidores civiles, ayuda a que la gestión de riesgos se integre en todos los niveles de la Entidad.

5.1.1.2 MARCO DE REFERENCIA

El marco de referencia de la Gestión Integral del Riesgo del RENIEC depende de su integración en la gestión de la entidad, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, principalmente de la Alta Dirección. En el RENIEC el marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la entidad.

A. Liderazgo y Compromiso

La Alta Dirección del RENIEC garantizan que la gestión integral del riesgo esté integrada en los objetivos estratégicos, que incluyen todas sus actividades de la entidad, de acuerdo con lo establecido en la política de la Gestión Integral del Riesgo que se alinea con las políticas existentes de los sistemas gestión y mejora continua en la entidad la SGEN y GG son responsables de la supervisión del desempeño de la Gestión Integral del Riesgo en coordinación con la Oficina de Integridad y Lucha contra la Corrupción.

B. Integración

La gestión integral del riesgo depende de la comprensión de las estructuras y el contexto de la entidad, es un proceso dinámico e iterativo, que se adapta a las necesidades y a la cultura de la entidad. En el RENIEC, los responsables de procesos y sistemas de gestión a cargo de alguna tipología de riesgos en la entidad, tienen la responsabilidad de tratar el riesgo según lo establecido en sus roles y responsabilidades.

C. Diseño

Comprende el análisis de los contextos interno y externo, teniendo en cuenta las situaciones del entorno de la Entidad y todas sus partes interesadas. La adecuada elaboración del contexto facilita la identificación, análisis, valoración, tratamiento (medidas de control), seguimiento y revisión, registro e informe de los riesgos.

- **El contexto interno**

  Comprender aquellos factores que podrían afectar el cumplimiento de los objetivos estratégicos de la entidad, para los cual es necesario identificar las debilidades y fortalezas (internas) que tienen cada uno de los procesos misionales, estratégicos y de soporte como una autoevaluación con la finalidad de lograr el cumplimiento de la misión en la entidad.

- **El contexto externo**

  Para los aspectos externos es importante poder reconocer las amenazas del medio y las oportunidades que se pueden presentar en cada uno de los procesos misionales, estratégicos y de soporte de la entidad y sobre todo saberlo manejar en función de la gestión del riesgo. Es importante resaltar que un buen análisis de contexto facilita una buena gestión del riesgo.

- **Articulación del Compromiso de la Gestión Integral del Riesgo**

  La Alta Dirección y los órganos del RENIEC articulan y demuestran su compromiso continuo con la gestión integral del riesgo mediante la aprobación y difusión de la política de Gestión Integral del Riesgo y objetivos.

- **Establecimiento de la comunicación y consulta**

  En el RENIEC, se establece un enfoque de comunicación y la consulta, para apoyar y facilitar la aplicación eficaz de la gestión integral del riesgo. La comunicación implica compartir información con todos los miembros de la organización y partes interesadas (Sistema Integrado de Tramite Documentario, correo electrónico institucional, intranet, micrositio, entre otros).

D. Implementación

El RENIEC ha implementado la gestión integral del riesgo mediante el desarrollo de un plan apropiado incluyendo plazos y recursos; la identificación cuándo, cómo y quién toma diferentes tipos de decisiones en toda la entidad; o la modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario; o el aseguramiento de que las disposiciones de la organización para gestionar los riesgos son claramente comprendidas y puestas en práctica. La implementación con éxito del marco de referencia requiere el compromiso y la toma de conciencia de todos los miembros de la organización y partes interesadas.

E. Valoración

A fin de valorar la eficacia del marco de referencia se considera: Medir anualmente el desempeño de la gestión integral del riesgo con relación a su propósito, plan de implementación, sus reportes y el comportamiento esperado para determinar si sigue siendo adecuado en la toma de decisiones y en el logro de los objetivos de la entidad.

F. Mejora

El RENIEC mejora continuamente la idoneidad, adecuación, eficacia y la manera en la que se integra el proceso de la gestión integral del riesgo. Sin embargo, cuando se identifiquen brechas u oportunidades de mejora pertinentes, desarrolla planes y tareas asignando a los responsables su implementación.

5.1.1.3 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.

La comunicación y consulta con las partes interesadas, externas e internas, se debe realizar en todas y cada una de las etapas del proceso de la Gestión Integral del Riesgo. Para ello, la Secretaría General y la Gerencia General, deben difundir la siguiente información:

a) La Política y Objetivos de la Gestión Integral del Riesgo y de Riesgos de Seguridad de la Información,
b) El Manual Gestión Integral del Riesgo, las Directivas y Manual de Seguridad de la Información.
c) El Plan de Gestión Integral del Riesgo y Plan de Acción Anual Medidas de Control aprobados por la Entidad, disponiendo su implementación.
d) Los resultados de avance de ejecución mensual del Plan de Gestión Integral del Riesgo y Plan de Acción Anual Medidas de Control.

Tabla N° 4: Comunicación Interna (Documentos Normativos)

¿Qué?	¿Cuándo?	¿A quién?	¿Cómo?	¿Quién?
Política y Objetivos de la Gestión Integral del Riesgo	Al ingreso del personal a la Entidad. Cuando se realizan modificaciones a la misma. De forma permanente	A los funcionarios y servidores de la Entidad	Página web e intranet. Comunicaciones Micro sitio de Control Interno Inducción a personal nuevo. SITD	SGEN/OSCD OILCC
Manual Gestión Integral del Riesgo	Cuando se realizan modificaciones a la misma. De forma permanente	A los funcionarios y servidores de la Entidad	Intranet. Sensibilización SITD	SGEN/OSCD OILCC

FUENTE: Elaboración OILCC

Tabla N° 5: Flujo de Comunicación Interna

¿Qué se debe comunicar?	¿Dónde se genera la información?	¿Quién debe comunicar?	¿A quién?	¿Cómo?	¿Cuándo?	Resultado
PAAMC y PGIR de los Productos priorizados y no priorizados)	Procesos	Gestor Líder de Riesgos.	Dueño del Proceso	SITD	Mensual	PGIR/PAAMC Aprobado por el Dueño del Proceso
PGIR/PAAMC Aprobado Por el Dueño del Proceso	Procesos	Dueño del Proceso	OILCC	SITD	Mensual	PGIR/PAAMC Evaluado por la OILCC y Oficiales de los sistemas de gestión

FUENTE: Elaboración OILCC

Los reportes que realiza la Entidad a la Contraloría General de la República, en el marco de la Gestión Integral del Riesgo es el Plan de Acción Anual – Medidas de Control - PAAMC.

Tabla N° 6: Flujo de Comunicación Externa

¿Qué se debe comunicar?	¿Dónde se genera la información?	¿Quién debe comunicar?	¿A quién?	¿Cómo?	¿Cuándo?	Resultado
PAAMC Aprobado por JNAC/SGEN	JNAC/SGEN	JNAC/SGEN	CGR	Aplicativo SCI - CGR	Al tercer y séptimo mes del año	PAAMC aprobado por JNAC/SGEN

FUENTE: Elaboración OILCC

5.1.2 REGISTRO E INFORME

El proceso de la Gestión Integral del Riesgo y sus resultados se debe documentar e informar. Para ello, el Dueño del proceso es responsable de: La elaboración, registro, actualización, disposición y custodia de la información documentada (físico y/o digital), relacionada al cumplimiento de la Gestión Integral del Riesgo.

Los registros utilizados para la Gestión Integral del Riesgo deben ser suscritos y firmados por los responsables de los órganos dueños de proceso que elaboran, revisan y aprueban. Así mismo, en dicho registro debe anotarse la fecha de elaboración y número de versión.

De acuerdo a los cambios en el contexto interno/externo, que motiven ajustes en la metodología de Gestión Integral del Riesgo o la herramienta de trabajo en formato Excel, utilizada para la aplicación metodológica, y en tanto se proceda a la actualización del presente documento, se podrá realizar actualizaciones de aspectos específicos, mediante la emisión de documentos de gestión a cargo del Órgano competente.

5.1.3 CRITERIOS PARA LA GESTIÓN INTEGRAL DEL RIESGO

Los criterios para la gestión de riesgos según la ISO 31000:2018 se basan en una serie de principios clave como la integración, la estructura, la personalización, la inclusión, la dinámica, la mejora continua, y la consideración de factores de riesgo, como el contexto externo e interno. Estos principios aseguran que la gestión del riesgo se alinee con los objetivos estratégicos de la entidad y se aplique en todos sus procesos. El RENIEC, de acuerdo a su estructura determina la cantidad y tipos de riesgo relacionados a sus productos y/o servicios.

5.1.3.1 Niveles de exposición y tolerancia al riesgo

La Entidad ha definido los niveles de probabilidad (baja, media, alta y muy alta) e impacto (bajo, medio, alto y muy alto), de cuyo producto (probabilidad por impacto), se obtiene el nivel de exposición al riesgo (bajo, medio, alto y muy alto). Al respecto, se ha establecido aceptar el nivel de exposición bajo, lo que implica que el dueño del proceso debe contar con acciones de seguimiento y revisión permanente.

Para el caso de las oportunidades, se ha definido los mismos niveles de probabilidad, impacto y nivel de exposición.

5.1.3.2 Decisión de tratamiento del riesgo (consideraciones)

Los riesgos de tipo operativo y seguridad de la información con niveles de exposición medio, alto y muy alto deben contar con un plan de tratamiento que incluya medidas de control o controles y acciones.

Los riesgos que afectan la integridad pública se dividen en dos, aquellos riesgos de tipo inconducta funcional tienen un nivel de exposición mínimo que va desde medio, alto a muy alto, mientras que los riesgos de tipo corrupción tienen un nivel de exposición mínimo de alto o muy alto. En ese sentido, el nivel de exposición bajo no existe para estos riesgos. Por ello, no pueden ser aceptados por la Entidad y deben pasar a la etapa de tratamiento.

Los riesgos identificados que se encuentran con un nivel de exposición superior al nivel aceptado por la Entidad, deben ser tratados, siguiendo el siguiente nivel de priorización:

- **MUY ALTO:** Requiere la adopción de medidas de control y acciones cuyo inicio de ejecución sea en el corto plazo.
- **ALTO:** Requiere la adopción de medidas de control y acciones cuyo inicio de ejecución sea en el corto o mediano plazo.
- **MEDIO:** Requiere la adopción de medidas de control y acciones que permitan disminuir el nivel de exposición al nivel aceptado por la entidad.

Por otro lado, las oportunidades identificadas deben ser aprovechadas siempre y cuando el nivel de exposición sea Alto o Muy Alto.

5.1.3.3 Cambios y modificaciones en el Plan de Acción Anual – Medidas de Control (PAAMC) y Plan de Gestión Integral del Riesgo (PGIR)

Si durante el seguimiento del PGIR/PAAMC, se identifica que las medidas de control no se vienen implementando de acuerdo a lo planificado o si se han presentado cambios en el entorno externo/interno que generan la variación del tratamiento del riesgo, el dueño del proceso debe desarrollar las siguientes acciones:

a) Evaluar el estado de avance del PGIR/PAAMC, analizando la problemática encontrada que dificulta el cumplimiento de la ejecución de las medidas de control para el tratamiento del riesgo, proponiendo las recomendaciones de mejora.

b) De identificarse nuevos riesgos, por cambios en el entorno externo/interno o producto del análisis del registro de situaciones adversas que se han materializado en los locales o unidades orgánicas, esto deberán ser incorporado en el PGIR/PAAMC, informando a la SGEN o GG, según corresponda con copia a la OILCC.

c) En el caso que el tratamiento para un determinado riesgo involucre a otro órgano se deberá coordinar previamente con los responsables de dichos órganos para su compromiso en la ejecución de las acciones de las medidas de control dentro de los plazos establecidos.

En el caso que el órgano responsable requiera realizar algún cambio en el PGIR difundido en la Entidad, se deberá emitir un documento formal dirigido a la SGEN o GG, según corresponda, con copia a la OILCC, justificando las razones de los cambios solicitados a fin de evaluar su pertinencia.

Por otro lado, en el caso que se requiera modificar el PAAMC aprobado por la Entidad, se deberá emitir un documento formal debidamente sustentado, dirigido a la SGEN o GG, según corresponda, con copia a la OILCC, que justifique los cambios solicitados, considerando que esta información es registrada en el aplicativo web de la Contraloría General de la Republica.

NOTA IMPORTANTE: Ante la presentación de algún cambio en el contexto interno o externo, así como cualquier situación adversa materializada que requiera realizar ajustes o modificaciones en los formatos Excel, establecidos por la OILCC para la gestión integral del riesgo y oportunidades, ésta será realizada por la OILCC, quien difundirá el formato actualizado a todos los órganos de la Entidad a través de un documento de gestión.

5.1.3.4 Planes para la gestión de riesgos

En la Entidad existen tres tipos de planes para gestionar los riesgos y se detallan a continuación:

- El Plan de Gestión Integral del Riesgo (PGIR) contiene todos los riesgos identificados por los dueños del proceso, con cualquier nivel de exposición (bajo, medio, alto o muy alto). Asimismo, registra el tratamiento que será otorgado para su reducción y/o mitigación. El plan se difunde de manera interna en la Entidad.
- El Plan de Acción Anual Medidas de Control (PAAMC) contiene todos los riesgos identificados por los dueños de los procesos que se encuentren vinculados a los productos priorizados,

aprobados por la Entidad, con cualquier nivel de exposición (bajo, medio, alto o muy alto). Asimismo, registra el tratamiento que será otorgado para su reducción y/o mitigación. Este plan se registra y reporta su avance, de manera periódica, a la Contraloría General de la República.

- El Plan de Gestión de Oportunidades (PGO) contiene las oportunidades identificadas por los dueños de los procesos con cualquier nivel de exposición (bajo, medio, alto o muy alto). Asimismo, registra el tratamiento que será otorgado para su aprovechamiento (perseguir la oportunidad) en el cumplimiento de los objetivos estratégicos institucionales. Este plan es de aplicación para aquellos sistemas de gestión que, por sus requisitos, lo requieran.

5.1.3.5 Normativa emitida por órganos rectores vinculada con la gestión de riesgos

- La Secretaría de Integridad Pública (SIP) es el órgano rector para establecer los lineamientos para fortalecer una cultura de integridad en las entidades del sector público, donde se incorpora la metodología para la gestión de riesgos que afectan la integridad pública (corrupción e inconducta funcional).
- La Contraloría General de la República (CGR) es el órgano rector para establecer los lineamientos para la implementación del Sistema de Control Interno, específicamente el eje gestión de riesgos.
- El Ministerio del Trabajo (MINTRA) es el órgano rector para establecer los lineamientos para la gestión de riesgos de Seguridad y Salud en el Trabajo, para lo cual la Entidad cuenta con un Comité de Seguridad y Salud en el Trabajo para establecer los lineamientos internos.
- La Secretaría de Gestión de Riesgos de Desastres de la Presidencia del Consejo de Ministros, a través del Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), implementa las políticas públicas para la gestión del riesgo de desastres (GRD). Para ello, nuestra Entidad cuenta con el responsable de riesgos de desastres de la Oficina de Seguridad y Defensa Nacional.

5.1.4 IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES EXISTENTES

La identificación de controles existentes es un paso fundamental en la gestión de riesgos, consiste en reconocer y documentar controles ya implementados en el proceso para evaluar si son suficientes o necesitan ser mejorados.

Los órganos dueños de procesos deben realizar la evaluación del control y/o controles existentes para todos los tipos de riesgos de acuerdo con los siguientes pasos:

- Paso 1: identificar el control o controles existentes, es decir, aquellos que se encuentran implementados y en uso dentro del proceso que está evaluando, utilizando los criterios establecidos en el anexo correspondiente. (Ver Anexo N° 1: Evaluación de Controles Existentes/Implementados)
- Paso 2: Evaluar cada uno de los controles, considerando los criterios establecidos en el registro de controles existentes (Ver Anexo N° 1: Evaluación de Controles Existentes/Implementados).
- Paso 3: Con el resultado de la evaluación del control existente, se valora la probabilidad e impacto del riesgo después de los controles existentes, con lo cual se obtendrá el denominado nivel de exposición del riesgo residual o riesgo después de los controles existentes. (Ver Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV), Anexo N° 5: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (hoja SIN_IAV) y Anexo N° 7: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA (hoja (INT_IAV)).

5.1.5 REEVALUACIÓN DE RIESGOS Y EFECTIVIDAD DE CONTROLES IMPLEMENTADOS

La reevaluación de riesgos es el proceso para determinar si las medidas de control implementadas han sido relevantes y efectivas al culminar el periodo de ejecución planificado, permitiendo que el riesgo residual, es decir, el riesgo después del tratamiento, alcance el nivel de tolerancia aceptado por la entidad (nivel Bajo).

Como parte del proceso de reevaluación de riesgos, en el caso que las medidas de control implementadas no hayan permitido reducir el nivel de exposición del riesgo al nivel aceptado, estos deben ser evaluados para su inclusión en un nuevo plan que será ejecutado en el siguiente periodo.

Durante la reevaluación de riesgos se puede identificar nuevos riesgos en el proceso que deban ser reducidos y/o mitigados a través de medidas de control, los cuales serán considerados en un nuevo plan que será ejecutado en el siguiente periodo.

Para el desarrollo de la presente actividad se hará uso del registro en formato Excel, para los riesgos operativos (Anexo N° 3: PLAN DE GESTIÓN INTEGRAL DEL RIESGO OPERATIVO – TRATAMIENTO (hoja (OPE_TR)), para los riesgos de seguridad de la información (Anexo N° 6: PLAN DE GESTIÓN INTEGRAL DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN – TRATAMIENTO (hoja (SIN_TR)) y para los riesgos que afectan la integridad pública (Anexo N° 8: PLAN DE GESTIÓN INTEGRAL DEL RIESGO QUE AFECTA LA INTEGRIDAD PÚBLICA – TRATAMIENTO (hoja (INT_TR)). Para ello, el gestor líder y equipo de riesgos/gestores operativos, deben realizar los siguientes pasos:

- Paso 1: Revisar el estado de ejecución de cada una de las medidas de control.
- Paso 2: Determinar, en caso el estado de la medida de control es "implementada", si la medida de control o control implementado ha permitido alguna de las siguientes alternativas:
  - Reducir el riesgo, hasta el nivel de tolerancia aceptado por la Entidad.
  - Reducir el riesgo, sin alcanzar el nivel de tolerancia aceptado por la Entidad.
  - No reducir el riesgo, manteniendo el mismo nivel de exposición.
  - No reducir el riesgo, permitiendo que se incremente el nivel de exposición.
- Paso 3: Fundamentar a través de un informe de resultado el análisis a través de información verificable, tales como: Reporte de incidencias, información estadística, reporte de disminución de salidas no conforme, reporte de disminución de reprocesos, entre otros.
- Paso 4: Revisar la información remitida por los dueños de los procesos, según el rol que corresponda: El oficial de calidad, en el caso de los riesgos operativos, el oficial de seguridad y confianza digital, en el caso de los riesgos de seguridad de la información o el responsable de la función de cumplimiento/antisoborno, con la finalidad de responder las siguientes preguntas:
  - ¿Cumplió con implementar la medida de control planificada?
  - ¿El nivel de probabilidad o impacto ha disminuido con la implementación de la medida de control?
  - ¿La justificación del órgano es coherente con la disminución de probabilidad o impacto?
- Paso 5: El oficial o responsable del sistema de gestión, según corresponda al tipo de riesgo, emiten una recomendación por cada medida de control, las cuales pueden ser:
  - No es efectivo - Requiere tratamiento adicional
  - Es efectivo - No requiere tratamiento adicional
- Paso 6: El oficial o responsable del sistema de gestión, según corresponda al tipo de riesgo, debe incluir un análisis adicional sobre la evaluación realizada.

5.1.5.1 Consideraciones para el riesgo residual

Culminada la reevaluación y efectividad de las medidas de control se deberá tener en cuenta lo siguiente:

a) En el caso que el nivel de exposición al riesgo después del tratamiento (riesgo residual) para los tipos de riesgo operativo y seguridad de la información, no se encuentre dentro de los niveles de exposición aceptados por la entidad (riesgo bajo), el dueño del proceso deberá realizar una evaluación del costo beneficio de adoptar nuevas medidas de control para su tratamiento en un siguiente periodo.

b) Luego de realizado el análisis costo beneficio para continuar el tratamiento de un riesgo identificado y este sea superior al

impacto en caso de su materialización, se deberá emitir un documento a la alta dirección, comunicando y sustentando la decisión de ACEPTAR el riesgo, manteniéndose bajo un continuo seguimiento.

5.1.6 IDENTIFICACIÓN DE RIESGOS PARA NUEVOS PRODUCTOS O SERVICIOS

Ante la propuesta de implementación de un nuevo producto o servicio en la entidad, se debe efectuar un análisis de gestión de riesgos, con la finalidad de garantizar, de manera razonable, la consecución de los objetivos, ante la presentación de eventos que podrían afectar de manera negativa el lanzamiento del nuevo producto o servicio. (Ver Anexo N° 9: REGISTRO PARA IDENTIFICACION DE RIESGOS EN NUEVOS PRODUCTOS, SERVICIOS O INICIATIVAS)

Esta metodología aplica a todas las fases, desde la conceptualización, diseño, desarrollo e implementación de cualquier nuevo producto, servicio o sistema de información que la Entidad decida implementar. El dueño del proceso y su equipo son los responsables de seguir los siguientes pasos:

- Paso 1: Identificar el proceso al cual se encuentra vinculado la propuesta de nuevo producto, servicio o iniciativa, así como el nombre del órgano responsable, nombre de la iniciativa del producto o servicio y la fecha en que se aprueba el registro de riesgo
- Paso 2: Registrar el tipo de riesgo identificado, que puede ser: Operativo, seguridad de la información o integridad.
- Paso 3: Registrar el riesgo identificado, de acuerdo a la metodología aprobada por la Oficina de Integridad y Lucha Contra la Corrupción
- Paso 4: Realizar un análisis de causas que podrían favorecer la materialización del riesgo identificado.
- Paso 5: Establecer los valores de probabilidad e impacto para calcular el nivel de exposición al riesgo
- Paso 6: Establecer las acciones para mitigar el riesgo identificado
- Paso 7: Registrar el resultado del seguimiento a la ejecución de las acciones establecidas para mitigar el riesgo.

NOTA IMPORTANTE: Los riesgos identificados durante el desarrollo de nuevos productos o servicios, así como la gestión de su tratamiento y monitoreo, debe ser presentada a la alta dirección para su conocimiento y gestión correspondiente.

5.1.7 REPORTE DE SITUACIONES ADVERSAS (RIESGO MATERIALIZADO)

Una situación adversa es un evento o incidente que ha ocurrido y se ha convertido en una falla o problema real en lugar de ser solamente una posibilidad futura, este evento puede causar pérdidas financieras, reputacionales, legales a la entidad y requieren de un análisis para entender sus causas y aplicar medidas correctivas para evitar que, en un futuro, vuelva a suceder. (Ver Anexo N° 10: REPORTE DE SITUACIONES ADVERSAS (RIESGO MATERIALIZADO))

Para identificar una situación adversa, se debe aplicar los siguientes criterios:

- El impacto o consecuencia de la materialización del riesgo ha afectado al menos uno de los objetivos estratégicos institucionales (fuga de datos; inconducta funcional, acto de corrupción, multas, sanciones por parte de órganos rectores, etc.).
- Se vea afectada la operatividad de una unidad, oficina o local de atención, interrumpiendo la prestación de servicios internos y externos.
- Ante la materialización de un evento crítico, es decir, la materialización de un riesgo, sea que este se encuentre o no dentro de los Planes de Gestión Integral del Riesgo o Plan de Acción Anual Medidas de Control (PGIR/PAAMC) el órgano dueño del proceso deberá remitir a la OILCC el formato correspondiente (ver Anexo N° 10: REPORTE DE SITUACIONES ADVERSAS (RIESGO MATERIALIZADO), el mismo que realizará los siguientes pasos:

Materializada una situación adversa, el órgano, unidad orgánica o local de atención adopta las acciones necesarias para mitigar las consecuencias de dicha situación. Asimismo, en el marco de la retroalimentación y con la finalidad de realizar una mejora en la gestión integral del riesgo, se debe reportar la siguiente información:

- Paso 1: Registrar la fecha y hora (aproximada) de la ocurrencia del hecho, así como el lugar donde se produjo la ocurrencia
- Paso 2: Registrar si el evento fue considerado, previamente, como un riesgo reportado en el Plan de Gestión Integral del Riesgo (PGIR) o el Plan de Acción Anual Medidas de Control (PAAMC), de ser afirmativo se consigna el código del riesgo asignado.
- Paso 3: Describir el evento, impacto o consecuencia, proceso afectado y controles vulnerados, así como las medidas que fueron adoptadas para mitigar el impacto del evento materializado.
- Paso 4: Remitir la información en el formato Excel establecido por la OILCC a través de un documento formal dirigido a la OILCC, con conocimiento del Oficial de Calidad y al Oficial de Seguridad y Confianza Digital.
- Paso 5: La OILCC en coordinación con el Oficial de Calidad y el Oficial de Seguridad y Confianza Digital, evaluarán el evento materializado con la finalidad de identificar riesgos en el ámbito de su competencia (riesgo operativo, seguridad de la información o integridad), pudiendo sugerir al órgano dueño del proceso su inclusión en el Plan de Gestión Integral del Riesgo, en el caso que dicho evento no se encuentre aun en el plan.

5.1.8 RIESGO ESTRATÉGICO

La gestión del riesgo estratégico se enfoca en la forma como se administra la entidad, en los asuntos globales relacionados a la visión, misión y cumplimiento de los objetivos estratégicos institucionales, así como la clara definición de políticas, el diseño y la conceptualización de la Entidad por parte de la Alta Dirección.

Los riesgos de tipo operativo, seguridad de la información y que afectan la integridad pública, identificados en los procesos de la entidad, constituyen el inventario de riesgos, principal fuente de información necesaria para la determinación de los riesgos de tipo estratégico. En ese sentido, corresponde a los dueños de los procesos con la asistencia técnica de los oficiales revisar el inventario de riesgos para identificar aquellos que pueden tener trascendencia institucional, para lo cual se debe tener en cuenta los siguientes criterios:

- **Cambio regulatorio o legal**: Una nueva ley o sentencia judicial que modifique **fundamentalmente** el rol, las responsabilidades o la estructura de financiamiento del RENIEC.
- **Disrupción tecnológica**: La Entidad tenga dificultades o imposibilidad técnica para lograr adoptar o integrar nuevas tecnologías de identidad (ejm. identidad descentralizada, biometría de última generación) a tiempo, volviendo sus productos o servicios obsoletos, vulnerables o ineficientes.
- **Cambios demográficos o migratorios:** Los cambios significativos en la población (ejm. alta tasa de migración, envejecimiento, disminución de natalidad, tasa de mortalidad) sobrepasen la capacidad operativa de las oficinas para mantener el registro actualizado y brindar los servicios con la calidad esperada.
- **Reputacional / Confianza pública:** Eventos externos (ejm. Voto golondrino, inscripciones no depuradas, brechas de seguridad informática, filtración de datos, suplantación) que erosionen la confianza en la información que proporciona el RENIEC.
- **Retención de talento especializado:** Dificultad de la entidad para atraer o conservar personal clave o altamente especializado (ejm. Especialistas en PKI, expertos en biometría, especialistas en identidad) debido a la competencia del sector privado o la inestabilidad del sector público.
- **Gestión de proyectos:** Los proyectos esenciales para el cumplimiento de la misión, visión u objetivos estratégicos institucionales de la Entidad (ejm. la masificación del DNIe, la interoperabilidad con otras entidades del estado, incorporación de actas registrales de las OREC) puedan exceder el presupuesto, el plazo de ejecución estimado, o no cumplir con el alcance planificado.
- **Integración de servicios:** Nuevas plataformas digitales de servicios no consigan interactuar de manera efectiva con los sistemas internos o los sistemas de entidades externas (ejm. SUNARP, sistema financiero, notarias, Poder Judicial, ESSALUD, programas sociales).

5.2 TIPOS DE RIESGO (OPERATIVO)

El riesgo operativo se define como la posibilidad de no cumplir el objetivo del proceso involucrado, afectando la calidad del producto o servicio, debido a fallas en los procesos, sistemas, personal o eventos externos que afecten las operaciones de la Entidad; este tipo de riesgo incluye errores humanos, procesos internos deficientes, entre otros.

5.2.1 IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden impedir o contribuir (oportunidades) a la Entidad en el logro de sus objetivos. Para ello, es importante contar con información veraz, apropiada y actualizada. Durante la identificación de los riesgos del proceso debe considerarse el análisis del contexto externo, interno y las partes interesadas, teniendo presente los objetivos y el alcance del proceso o producto (priorizado o no priorizado), servicio, sistema de gestión u otros. En ese sentido, debemos considerar las técnicas existentes para la identificación de riesgos (Ishikawa, causa efecto, diagrama de procesos, cinco por qué, observación, marco lógico, lluvia de ideas, entre otras) que mejor se adapten a las capacidades del personal, así como a la naturaleza y grado de incertidumbre de los riesgos. Para ello, el gestor líder junto al equipo de riesgos/gestores operativos deben seguir los siguientes pasos:

- Paso 1: Seleccionar la técnica a emplear para la identificación de riesgos en su proceso, según la siguiente tabla:

TABLA N° 7: TÉCNICAS UTILIZADAS EN LA GESTIÓN DEL RIESGO

ITEM	HERRAMIENTA	DESCRIPCION
1	Luvia o tormenta de ideas	Técnica cualitativa, efectiva para generar ideas nuevas.
2	Entrevistas estructuradas o semiestructuradas	Entrevistar a participantes experimentados e interesados en la materia de riesgos, así como aquellos funcionarios involucrados en los principales procesos.
3	Delphi	Es un método para predecir el futuro utilizando expertos en el área a la cual pertenece el problema.
4	Análisis de flujo de procesos y preliminar de riesgos	Por cada proceso se debe implementar la representación esquemática del mismo, con el objetivo de visualizar la interrelación entre las entradas, tareas, salidas y responsabilidades en relación a los componentes del Sistema de Control Interno por cada proceso alineado a sus objetivos y metas por cada nivel jerárquico y/o unidad orgánica dependiendo del caso.
5	Estudios de peligro y operatividad (HAZOPP)	Sistema de procedimientos e instrumentos para una planificación de proyectos orientada a objetivos. Zopp es el método final de panificación de proyectos. Características Procedimiento de planificación por pasos sucesivos Visualización y documentación permanente de los pasos de planificación.
6	Apreciación de riesgos ambientales	Son métodos para escoger alternativas a situaciones de prevención en respuesta a la responsabilidad social institucional y proyección a la preservación del medio ambiente.
7	Análisis de causa primordial (análisis de daño único)	Centra su análisis en los factores internos y externos que han dado, o pueden dar lugar, a eventos negativos (riesgos).
8	Análisis de modos de fallo de los efectos	Un método eficaz de combinar conceptos de probabilidades y valor (o satisfacción) esperados en la solución de problemas complejos que involucran tanto incertidumbre como un gran número de alternativas.
9	Análisis causa y efecto (Ishikawa)	Es una representación gráfica que muestra la relación cualitativa e hipotética de los diversos factores que pueden contribuir a un efecto o fenómeno determinado. Resulta útil para identificar las causas de los riesgos, hasta llegar a la causa raíz.
10	Mantenimiento centrado en la fiabilidad	Como consecuencia del proceso de implementación de la gestión integral del riesgo y detectados los eventos de riesgo, una manera de visualizar, representar y comprender de manera gráfica la incertidumbre del riesgo, es centrándonos en un escenario flexible al cambio aplicable al contexto interno o externo de los objetivos, con la finalidad de identificar cuáles son los múltiples eventos que afectan su logro en el tiempo.
11	Índices de alarma y de riesgo	Dada la implementación del flujo del proceso, identificamos los principales indicadores de eventos de riesgo. Estas, son mediciones cualitativas y/o cuantitativas que proporcionan un mayor conocimiento de la amenaza o debilidad del compromiso del RENIEC con el cumplimiento de los objetivos institucionales.

12	Matriz consecuencia probabilidad / eventos que pueden afectar objetivos.	Es un instrumento muy utilizado que muestra los posibles resultados que se pueden conseguir, al seguir cursos alternativos de acción (estrategias) en diferentes circunstancias.
13	Análisis de costos/beneficios y cadena de valor	Esta técnica permite, nos da el enfoque visual del conjunto de actividades que abarca: la logística de compras, que se refiere a la obtención de los insumos o servicios adecuados en términos de calidad, cantidad, precio, tiempo y lugar; ii) la producción, que atañe a la transformación de los insumos en productos finales; iii) la logística de ventas, que comprende las actividades de almacenamiento y distribución de tales productos, para que puedan estar disponibles en términos de calidad, cantidad, precio, tiempo y lugar adecuados; iv) el marketing y la comercialización, que involucran la elaboración y ejecución de la estrategia de venta de bienes o servicios; y v) la atención al cliente, que se refiere al servicio que prestan las empresas a sus clientes para solicitar información y asistencia técnica, manifestar reclamos, y efectuar devoluciones, entre otros. A medida que los materiales (insumos y productos finales) avanzan en los diferentes nodos de la cadena, diferentes funciones y procesos les agregan valor, con el objetivo de lograr el mayor valor agregado al menor costo.

FUENTE: Elaboración OILCC

- Paso 2: Identificar el objetivo del proceso, el producto, sus atributos y oportunidades, de acuerdo al modelo de gestión por procesos de la Entidad a cargo de la Unidad de Modernización Organizacional de la Oficina de Planificación, Presupuesto y Modernización.
- Paso 3: Identificar las actividades del proceso de acuerdo al inventario de procesos de la Entidad, difundido por la Unidad de Modernización Organizacional de la Oficina de Planificación, Presupuesto y Modernización.
- Paso 4: Identificar los riesgos utilizando las preguntas guía que se encuentran en la siguiente tabla:

TABLA N° 8: PREGUNTAS GUIA PARA LA IDENTIFICACION DE RIESGOS	
1	¿Qué puede ocurrir?
2	¿Cómo puede suceder?
3	¿Quién puede generarlo?
4	¿Por qué se puede presentar?
5	¿Cuándo puede ocurrir?
6	¿Qué efectos (consecuencias) traería su ocurrencia?
7	¿Cuáles son los factores, situaciones o eventos que podrían afectar negativamente el cumplimiento de los objetivos del proceso, producto o servicio?
8	¿Cuáles son los factores, situaciones o eventos que podrían afectar en mayor medida el cumplimiento de plazos y estándares del proceso, producto o servicio?

FUENTE: Elaboración OILCC

- Paso 5: Identificar las causas que originan el riesgo y los efectos que podrían presentarse en caso se materialice. (Ver Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV)).
- Paso 6: Formular y redactan los riesgos que afectan a sus procesos, considerando los siguientes elementos: **[Producto o servicio + Verbo en condicional simple (Podría) + Evento adverso + Efecto].** Por

ejemplo: "El DNI electrónico de mayor de edad podría entregarse fuera del plazo establecido ocasionando quejas, reclamos o denuncias ante órganos rectores, afectando la imagen de la entidad o ser pasivo de sanciones**".** (Ver Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV)).

- Paso 7: El gestor líder junto al dueño del proceso revisan y validan la identificación de los riesgos en el proceso. (Ver Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV)).

5.2.2 ANÁLISIS Y VALORACIÓN DEL RIESGO

El análisis del riesgo es el proceso para comprender la naturaleza del riesgo y determinar su nivel de exposición, proporciona la base para la valoración del riesgo y para las decisiones sobre su tratamiento. Para ello, el gestor líder junto al equipo de riesgos/gestores operativos deben emplear el registro en formato Excel (Ver Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV)) y seguir los siguientes pasos:

- Paso 1: Estimar la frecuencia que el evento de riesgo ocurra, se mide como: Baja, Media, Alta o Muy Alta.

TABLA N° 9: NIVELES DE PROBABILIDAD PARA RIESGOS OPERATIVOS		
CLASIFICACION	**NIVEL**	**DESCRIPCION Y FRECUENCIA**
BAJA	4	El riesgo podría ocurrir rara vez sólo en circunstancias excepcionales o en un horizonte aproximado mayor a un año.
MEDIA	6	El riesgo puede ocurrir en algún momento relativamente frecuente o en un futuro cercano menor a un trimestre.
ALTA	8	El riesgo puede ocurrir en la mayoría de las circunstancias o aproximadamente una vez al mes.
MUY ALTA	10	El riesgo podría ocurrir en la mayoría de las circunstancias en un presente muy cercano o aproximadamente en días.
Fuente: DI-006-2019-CG/INTEG		
Nota importante: El análisis de la probabilidad basado en la frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos y estadísticos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y del análisis de sus factores internos y externos.		

FUENTE: Elaboración OILCC

- Paso 2: Estimar el impacto y las consecuencias si el riesgo se materializa, se mide como: bajo, medio, alto o muy alto

TABLA N° 10: NIVELES DE IMPACTO PARA RIESGOS OPERATIVOS					
Impacto	Nivel	Criterios a considerar para medir el impacto del riesgo			
		Objetivos Estratégicos Institucionales	Cumplimiento legal y normativo	Reputacional	Operatividad
BAJO	4	No hay consecuencias o sus efectos son insignificantes en los resultados y objetivos estratégicos institucionales.	No ocasiona incumplimiento legal o normativo. No existe posibilidad de sanciones, demandas, observaciones-recomendaciones de auditorías, o similares.	Las consecuencias ocasionan un impacto que no es percibido por los grupos de interés o el cliente interno	No se interrumpe la operatividad. Las consecuencias pueden ser asimiladas dentro de las actividades del proceso.
MEDIO	6	Las consecuencias afectan medianamente a los resultados o a los objetivos estratégicos institucionales.	Incumplimiento legal o normativo de impacto medio. Hay posibilidad de penalidades, multas o sanciones menores, observaciones o recomendaciones de auditorías, o similares.	Las consecuencias son percibidas por el cliente ciudadano, el cliente interno u otros grupos de interés, afectando medianamente la reputación de la Entidad, a través quejas, reclamos, denuncias o similares.	Existen interrupciones de corta duración en la operatividad y las consecuencias pueden afectar al proceso o a sus principales actividades por un corto plazo, disminuyendo la producción esperada.
ALTO	8	Las consecuencias afectan de manera considerable los resultados y objetivos estratégicos institucionales.	Incumplimiento legal o normativo de impacto grave. Hay fuertes penalidades, multas o sanciones, observaciones o recomendaciones de auditorías, o similares.	Las consecuencias afectan significativamente a la reputación de la Entidad, son percibidas por los grupos de interés. Se originan quejas, reclamos, denuncias o similares a través de medios de comunicación masiva o redes sociales	Existe interrupción parcial prolongada de la operatividad, afectando a uno o mas procesos, productos o servicios de la Entidad.
MUY ALTO	10	Las consecuencias afectan de manera grave o importante la consecución de los resultados y objetivos estratégicos institucionales o el cumplimiento de la misión institucional	Incumplimiento legal o normativo de impacto muy alto. Se presentan multas o sanciones, no conformidades de auditorías, o similares.	Las consecuencias afectan de manera grave a la reputación de la Entidad ante los grupos de interés. Se apertura procesos sancionadores contra la entidad por organismos reguladores u otros poderes del estado	Existe una interrupción prolongada de la operatividad, afectando a varios procesos, productos o servicios de la Entidad.

FUENTE: Elaboración OILCC

- Paso 3: Calcular el nivel de exposición al riesgo (riesgo inherente), se expresa como la combinación de la probabilidad de ocurrencia y el impacto de las consecuencias. Se mide como: Bajo, Medio, Alto o Muy Alto. En el caso de los riesgos operativos el nivel de exposición "Bajo" es aceptado por la Entidad, mientras los demás niveles de exposición requieren pasar a la etapa de tratamiento.
- Paso 4: Registrar la información, en caso corresponda, del código y descripción de controles existentes), aquellos que pueden disminuir la probabilidad o impacto de ocurrencia del riesgo inherente.

La valoración del riesgo consiste en comparar los resultados del análisis del riesgo (el nivel de riesgo) con los criterios del riesgo establecidos previamente para determinar si el riesgo y su impacto o consecuencia es aceptable o tolerable por la Entidad y si requiere una acción adicional, es decir, pasa a la etapa de tratamiento del riesgo. El propósito es apoyar la toma de decisiones. Para ello, el gestor líder junto al equipo de riesgos/gestores operativos deben emplear el registro en formato Excel. (Ver Anexo N° 2: PLAN DE GESTIÓN

INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS (hoja OPE_IAV)) y seguir los siguientes pasos:

- Paso 1: Considerar el resultado de la evaluación del control existente, sirve como insumo para la valoración de la probabilidad e impacto del riesgo inherente.
- Paso 2: valorar la probabilidad e impacto de la materialización del riesgo inherente con los controles existentes, pudiendo esta disminuir o mantenerse.
- Paso 3: Calcular el nivel de exposición al riesgo (riesgo residual), se expresa como la combinación de la probabilidad de ocurrencia y el impacto de las consecuencias. Se mide como: Bajo, Medio, Alto o Muy Alto.
- Paso 4: De acuerdo al nivel de exposición al riesgo residual, se realiza la comparación con los criterios del riesgo definidos y se elige la opción de tratamiento, pudiendo ser: Evitar, reducir, compartir o aceptar. Teniendo en cuenta la política de gestión de riesgos de la Entidad, considerando que en el caso de los riesgos operativos el nivel de exposición "Bajo" es aceptado, mientras los demás niveles de exposición requieren pasar a la etapa de tratamiento.

TABLA N° 11: CRITERIOS PARA LA RESPUESTA AL RIESGO EN LA ETAPA DE TRATAMIENTO

NIVEL DE EXPOSICION	ALTERNATIVAS DE RESPUESTAS	CRITERIO
RIESGO MUY ALTO	EVITAR, REDUCIR O COMPARTIR	Los riesgos con nivel de exposición muy alto requieren una gestión prioritaria y una respuesta inmediata y coordinada con los órganos involucrados. Para ello, deben contar con medidas de control eficientes y efectivas, así como un Plan de contingencia u otro plan similar, que permita asegurar una oportuna recuperación ante la materialización del riesgo. Se debe informar de manera permanente a la Alta dirección del avance en el tratamiento.
RIESGO ALTO	EVITAR, REDUCIR O COMPARTIR	Los riesgos con nivel de exposición alto requieren de una gestión prioritaria y una respuesta planificada a través de medidas de control eficientes y efectivas que permitan reducir los niveles de exposición. Para ello, pueden establecer planes de contingencia debidamente aprobados e informados a la Alta dirección.
RIESGO MEDIO	REDUCIR O COMPARTIR	Los riesgos de nivel medio se tratan con medidas de control para reducir su nivel de exposición a la zona de riesgo aceptado por la Entidad. Se aplican acciones preventivas y/o correctivas según corresponda, teniendo en cuenta la relación costo/beneficio del tratamiento.
RIESGO BAJO	ACEPTAR	Los riesgos con este nivel se encuentran dentro del límite de tolerancia aceptado por la Entidad. En este caso, se puede mantener los controles existentes. La materialización de este tipo de riesgos no representa un peligro elevado para la entidad, o partes interesadas; sin embargo, requieren ser monitoreados por el órgano dueño del proceso a través de procedimientos rutinarios para garantizar que el nivel del riesgo se mantenga bajo control.

FUENTE: Elaboración OILCC

5.2.3 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo consiste en la planificación y ejecución de medidas de control o controles y acciones, con el objetivo de reducir o mitigar la probabilidad de ocurrencia o el impacto negativo en caso se produzca. Este

proceso implica la selección de estrategias de tratamiento a implementar. Para ello, el gestor líder junto al equipo de riesgos/gestores operativos deben emplear el registro en formato Excel, (Ver Anexo N° 3: PLAN DE GESTIÓN INTEGRAL DEL RIESGO OPERATIVO – TRATAMIENTO (hoja OPE_TR)) y seguir los siguientes pasos:

- Paso 1: Ingresar el código del riesgo con la finalidad que, de manera automática, se complete la información relacionada al mismo, como: si corresponde al PGIR o PAAMC, el código en caso que sea un riesgo del PAAMC, la descripción del riesgo, las causas, efectos, nivel del riesgo residual y su valoración.
- Paso 2: Registrar la información de la medida de control alineada a cada una de las causas identificadas, señalando: código de medida de control, descripción de la medida, órgano responsable (involucrado), fecha de inicio y fin de implementación, así como el medio de verificación que sustentara la implementación de la medida de control.
- Paso 3: Registrar la información de las acciones alineadas a la implementación de cada una de las medidas de control consignadas, señalando: código de la acción, descripción de la acción, órganos involucrados, fecha de inicio y fin de implementación y medio de verificación que sustentara la implementación de la acción.

5.2.4 REMISIÓN Y APROBACIÓN DEL PGIR/PAAMC

La aprobación del plan de Gestión Integral del Riesgo (PGIR) y Plan de Acción Anual Medidas de Control (PAAMC), implica la ratificación formal del plan que contiene los riesgos identificados y las estrategias para mitigarlos. Para ello, se deben seguir los siguientes pasos:

- Paso 1: El dueño del proceso, revisa y aprueba el PGIR/PAAMC del proceso a su cargo, con la finalidad de remitirlo al Oficial de Calidad para su revisión.
- Paso 2: El Oficial de Calidad revisa y, de corresponder, realiza la validación y retroalimentación correspondiente al órgano dueño del proceso para los ajustes pertinentes. Una vez revisado, remite el plan al dueño del proceso para su firma.
- Paso 3: El dueño del proceso remite la versión final del PGIR/PAAMC, aprobada y firmada a la OILCC para su consolidación y, en el caso del PAAMC, su registro en el aplicativo informático del SCI de la CGR
- Paso 4: La OILCC remite el PGIR/PAAMC a la Secretaría General o Gerencia General, según el órgano de procedencia, con la finalidad que sea aprobado y difundido en la Entidad.

5.2.5 EJECUCIÓN Y SEGUIMIENTO DEL PGIR/PAAMC

La ejecución comprende la implementación de las acciones y medidas de control consignadas en el PGIR/PAAMC, orientadas a la reducción o mitigación de los riesgos que se encuentran en la etapa de tratamiento. Esta actividad es desarrollada por los órganos dueños del proceso y reportada de

manera mensual a la OILCC, adjuntando las evidencias que corroboren el avance progresivo.

El seguimiento se encuentra a cargo del Oficial de Calidad, quien monitorea de manera mensual la ejecución de las acciones y medidas de control consideradas en el PGIR/PAAMC, el seguimiento permite determinar el estado de ejecución de cada una de las acciones y medidas de control consignadas, sobre la base de la información y documentación que proporcionada por los órganos dueños del proceso. El estado de ejecución de las medidas de control se determina considerando los siguientes criterios:

TABLA N° 12: ESTADO DE LA MEDIDA DE CONTROL

Estado	Criterio
Implementada	Cuando el responsable ha cumplido con implementar la medida de control conforme al PGIR/PAAMC.
No implementada	Cuando el responsable no ha cumplido con implementar la medida de control contenida en el PGIR/PAAMC y el plazo para su ejecución ha culminado definitivamente.
En proceso	Cuando el responsable ha iniciado, pero aún no ha culminado con la implementación de la medida de control contenida en el PGIR/PAAMC
Pendiente	Cuando el responsable no ha iniciado la implementación de la medida de control contenida en el PGIR/PAAMC.
No aplicable	Cuando la medida de control contenida en el PGIR/PAAMC, no puede ser ejecutada por factores no atribuibles al dueño del proceso, debidamente sustentados, que imposibilitan su implementación.
Desestimada	Cuando el responsable decide no implementar la medida de control contenida en el PGIR/PAAMC, asumiendo las consecuencias de dicha decisión.

FUENTE: Elaboración OILCC

En ese sentido, el Gestor Líder junto al equipo de riesgos/gestores operativos, debe emplear el registro en formato Excel, hoja OPE_TR y seguir los siguientes pasos:

- Paso 1: El Gestor Líder y equipo de riesgos/gestores operativos ejecutan las acciones asociadas a cada medida de control vinculada a los riesgos operativos identificados. Registran el avance mensual y adjuntan las evidencias que corresponden.
- Paso 2: El órgano dueño del proceso traslada el avance de ejecución al Oficial de la Calidad con conocimiento de la OILCC.
- Paso 3: El Oficial de la Calidad junto a su equipo de trabajo revisa y valida el avance reportado por el órgano dueño del proceso, conforme a los medios de verificación remitidos. Comunica el resultado a la OILCC.
- Paso 4: La OILCC consolida la información remitida por el Oficial de la Calidad e incorpora los avances obtenidos en el informe de resultado mensual que remite a la Secretaría General y Gerencia General con la

finalidad que tomen conocimiento de los avances obtenidos por los órganos dueños de los procesos.

- Paso 5: La OILCC comunica a los órganos dueños de los procesos, mediante correo electrónico, los avances y comentarios consignados por el Oficial de la Calidad.
- Paso 6: La Secretaría General o Gerencia General, según corresponda, toman conocimiento de lo expuesto en el informe de resultado remitido por la OILCC.

5.2.6 IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN Y TRATAMIENTO DE OPORTUNIDADES

La norma ISO 31000 (Gestión del Riesgo - Directrices) define el riesgo como el "efecto de la incertidumbre sobre los objetivos", este efecto puede ser una desviación positiva o negativa de lo que se espera. Las oportunidades son, el lado positivo de esa incertidumbre, es decir, la posibilidad que un evento o circunstancia genere un resultado favorable que permita alcanzar o superar los objetivos del proceso y los objetivos estratégicos institucionales.

La gestión de oportunidades en la entidad, busca capitalizar los riesgos positivos que surgen en un entorno dinámico. Se concentra en gestionar la incertidumbre del entorno operativo para mejorar sus productos y servicios en el cumplimiento de su misión, entre otros. Por ejemplo: Implementación de nuevas tecnologías, Inteligencia Artificial o cadena de bloques, desarrollar o mejorar plataformas virtuales, convenios de interoperabilidad de datos con otras entidades públicas.

Para el tratamiento de las oportunidades se debe priorizar aquellas que, luego de ser evaluadas, se encuentren en los niveles de exposición **"Alto"** o **"Muy Alto**". Asimismo, se debe considerar que en el camino a su aprovechamiento se puede presentar riesgos asociados, los cuales deberán ser identificados.

Para identificar, analizar, valorar y tratar las oportunidades se debe utilizar el registro del Plan de Gestión de Oportunidades

5.3 TIPOS DE RIESGO (SEGURIDAD DE LA INFORMACION)

El riesgo de seguridad de la información se refiere a la posibilidad de que amenazas exploten vulnerabilidades de los activos de información de los procesos de la institución, afectando la confidencialidad, integridad y disponibilidad. Estos riesgos pueden surgir de diversas fuentes incluyendo ataques cibernéticos, errores humanos, fallos técnicos y desastres naturales.

5.3.1 IDENTIFICACIÓN DE ACTIVOS DE INFORMACION

Para la identificación de activos de información, el Órgano dueño del proceso y su equipo, en coordinación del Oficial de Seguridad y Confianza Digital, registra en el formato para inventario de activos de información (Ver Anexo N° 4: INVENTARIO DE ACTIVOS DE INFORMACIÓN (Hoja Inv_Act) para lo cual debe realizar lo siguiente:

- Paso 1: Asignar un código de activo, nombre de la unidad orgánica responsable, proceso involucrado, nombre y descripción del activo.
- Paso 2: Registrar el tipo de activo (Información, Software, Físico, Personas o Servicios) y categoría del activo, así como su ubicación física o lógica, según corresponda. Además, se registra la ubicación especifica, propietario y custodio del activo.
- Paso 3: Se registra la frecuencia de uso del activo de información (Diario, semanal, quincenal, mensual, anual o eventual).
- Paso 4: Se registra el nivel de afectación de acuerdo a los principios de seguridad de la información (Confidencialidad, Integridad y Disponibilidad), que pueden ser: Baja, media o alta, para obtener el nivel de valoración del activo que puede ser: No significativo, menor, moderado, critico o muy crítico.

TABLA N° 13: VALORACION DEL ACTIVO POR EL PRINCIPIO DE CONFIDENCIALIDAD

Valor	Clasificación	Criterio	Consecuencia
3	Alta	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce daños de gran magnitud, como lo son: - Pérdida de la ventaja competitiva. - Uso malicioso en contra del RENIEC. - Pérdidas financieras que no pueden ser absorbidas por el RENIEC. - Demandas legales que dañan la imagen y confianza pública del RENIEC.
2	Media	Es la información que debe ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas.	La divulgación no autorizada produce daños de mediana magnitud, como lo son: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por el RENIEC. - No se producen demandas legales.
1	Baja	Es la información que puede ser divulgada a público general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para el RENIEC.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

TABLA N° 14: VALORACION DEL ACTIVO POR EL PRINCIPIO DE INTEGRIDAD

Valor	Clasificación	Criterio	Consecuencia
3	Alta	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: - Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). - Daño de la imagen del RENIEC (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.

2	**Media**	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: - Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). - Daño de la imagen del RENIEC (daño a nivel regional o nacional, pudiéndose reparar en el corto plazo). - No se pierde la confianza de los usuarios.
1	**Baja**	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: - Pérdidas económicas (no impacta las ganancias, se cumplen las metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo, pero este es manejable). - Daño de la imagen del RENIEC (daño a nivel nacional o regional que puede no ser percibido y se puede reparar prontamente). - No se pierde la confianza de los usuarios.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

TABLA N° 15: VALORACION DEL ACTIVO POR EL PRINCIPIO DE DISPONIBILIDAD

Valor	Clasificación	Criterio	Consecuencia
3	**Alta**	Es información o activo indispensable para la continuidad del RENIEC. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: - Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. - Perjuicios legales que afectan la imagen del RENIEC. - Perjuicios económicos que no pueden ser absorbidos por el RENIEC. - Problemas sindicales.
	Media	La disponibilidad de la información es necesaria para la continuidad del RENIEC, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.	La falta de disponibilidad por periodos prolongados produce: - Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. - Perjuicios legales que no comprometen la imagen del RENIEC. - Perjuicios económicos que pueden ser absorbidos por el RENIEC. - No hay problemas sindicales.
1	**Baja**	Es información o activos de apoyo o secundarios para el negocio. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes.	Falta de disponibilidad, sin importar el periodo de tiempo, produce: - Que los niveles de servicio acordados para los procesos operativos importantes, no se ven afectados. - Problemas administrativos y operativos no significativos. - Perjuicios económicos que no son significativos. - No hay perjuicios legales. - No hay problemas sindicales.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

- Paso 5: Con base a los criterios anteriores se clasifica el activo de información, que puede ser: Publico o confidencial.

TABLA N° 16: CLASIFICACION DE LA INFORMACION		
Nro.	**Clasificación de Información**	**Definición**
1	**Público**	Todo documento en cualquier formato que se encuentre en poder de las Instituciones públicas. Toda información que puede ser conocida por el público en general. Su difusión no representa riesgo alguno para la continuidad de las operaciones del RENIEC.
2	**Confidencial**	Consejos, recomendaciones u opiniones previas a la toma de una decisión del RENIEC, salvo que sea pública. Información bancaria, tributaria, comercial, industrial, tecnológica y bursátil regulada por la legislación pertinente. Datos personales (invade la intimidad personal o familiar). Información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la administración pública. Información preparada u obtenida por asesores jurídicos o abogados que pudieran revelar la estrategia en la tramitación o defensa en un proceso administrativo o judicial. Su difusión o uso no autorizado puede representar riesgos al proceso y/o incumplimiento de las normas legales.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

- Paso 6: Se registra la información de etiquetado del activo, así como el estado del mismo, relacionado a su situación o fecha de baja.
- El etiquetado de activo, en relación con seguridad de la información se refiere asignar etiquetas o marcas identificativas a los activos de información, con el fin de clasificarlos según su nivel de confidencialidad identificado. Para el etiquetado se debe considerar lo siguiente: *"Según lo definido en el inventario de activos de información, se etiquetarán los activos clasificados como confidencial. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico, electrónico y digital con la siguiente exclusión: No se etiqueta las bases de datos, ni reportes o salidas de los sistemas de información o sistemas informáticos, sin embargo, se establecen los controles de seguridad necesarios."*

5.3.2 IDENTIFICACIÓN DEL RIESGO

Para la identificación de riesgos, el órgano dueño del proceso y su equipo, en coordinación del Oficial de Seguridad y Confianza Digital, registran en el formato (Ver Anexo N° 5: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (Hoja SIN_MR) la siguiente información:

- Paso 1: Se registra la siguiente información en la cabecera del registro:
  - Fecha de Elaboración: La fecha en la que se realiza o se actualiza la matriz.

- Tipo de Proceso: El proceso al que pertenece en función al “Mapa de Procesos de Nivel 0 y 1”, donde se realiza el levantamiento de activos de información, por ejemplo: Misional, Estratégico, Soporte
- Proceso Nivel 0: El proceso al que pertenece en función al “Mapa de Procesos de Nivel 0 y 1”, donde se realiza el levantamiento de activos de información
- Órganos Dueño del Proceso: El Órgano Dueño del proceso, donde se realiza la identificación de riesgos
- Órganos que participan en el proceso: Los órganos que participan en el proceso.

- Paso 2: Tomando en cuenta el formato del “Inventario de Activos de Información”, aquellos activos que fueron valorados como “Crítico” y “Muy Crítico”, pasan a la evaluación de riesgos de seguridad de la información, inicialmente para la identificación de riesgos de Seguridad de la Información.
- Paso 3: Se registra la siguiente información de la etapa de identificación: Datos Generales tales como:
  - Código del riesgo: Para identificar los activos de información a través de la siguiente codificación: Código del Proceso (Iniciales) + SIN + R+ número correlativo. Ejemplo: PM01.01-SIN-R01 o PM02-SIN-R26
  - Origen: El medio a través del cual se identifica el riesgo, estos pueden ser:
    - Matriz FODA: Relacionado a las cuestiones internas y externas de la entidad.
    - Matriz de Partes Interesadas: Relacionado a las necesidades y expectativas de las partes interesadas.
    - Ejecución de actividades: Relacionado al desarrollo de tareas del proceso.
  - Producto: registra de acuerdo a la gestión por procesos
  - Identificación del riesgo
    - Activo: Registra el activo que se identificó como “Muy Crítico” y “Crítico” en el “Inventario de Activos de Información”.
    - Amenaza: Registrar, teniendo en cuenta como base la tabla “Lista de amenazas (ISO 27005)”

TABLA N° 17: LISTA DE AMENAZAS (SEGÚN LA NORMA ISO 27005)

TIPO	EJEMPLO
Amenaza física	*Fuego*
	Amago de incendio
	Aniego
	Contaminación
	Accidente grave
	Explosión
	Polvo
	Corrosión

	Congelamiento
Eventos naturales	*Terremoto*
	Inundación
	Pandemia
Falla de infraestructura	*Falla del suministro eléctrico*
	Falla del sistema de ventilación o enfriamiento
	Falla de la red informática
	Falla del equipo de red
Fallas técnicas	*Falla del sistema o software*
	Saturación del sistema o software
	Falla en el mantenimiento del sistema o software
	Ciberataque
Acciones humanas	*Huelgas*
	Manifestaciones
	Ingeniería social
	Escucha indebida
	Robo de equipo
	Robo de documentos
	Robo de credenciales
	Filtración indebida de datos
	Revelación de información
	Entrada de datos no confiable
	Manipulación de hardware
	Manipulación de software
	Ataque de hombre en el medio
	Tratamiento no autorizado de datos personales
	Entrada no autorizada a los ambientes
	Uso no autorizado de los equipos
	Uso incorrecto de los equipos
	Daño de los equipos
	Copia ilegal o pirata
Compromiso de funciones o servicios	*Error de datos*
	Abuso de derechos o permisos
Amenazas organizacionales	*Falta de personal*
	Falta de equipos
	Falta de espacio físico
	Infraestructura no cumple las normas de edificaciones
	Infraestructura no cumple las normas de defensa civil

FUENTE: Norma ISO 27005

- Vulnerabilidad: Registrar, teniendo en cuenta la tabla (Lista de vulnerabilidades (ISO 27005))

TABLA N° 18: LISTA DE VULNERABILIDADES (ISO 27005)	
TIPO	**VULNERABILIDAD**
Hardware	Mantenimiento insuficiente de equipos
	Mantenimiento de equipos sin planificación
	Susceptibilidad a la humedad
	Susceptibilidad al polvo
	Susceptibilidad al calor
	Equipos desprotegidos
	Equipo desatendido
	Servidor fuera del Data Center
	Equipo utilizado fuera de los parámetros de uso (por ejemplo, uso continuo)
Software	Pruebas de software nulas o insuficientes
	Defectos conocidos en el software
	Sin "Cierre de sesión" al salir de la estación de trabajo
	Reutilización de equipos sin el formateo o borrado respectivo
	Configuración insuficiente de registros para fines de seguimiento de auditoría
	Asignación incorrecta de derechos de acceso
	Interfaz de usuario complicada
	Insuficiente o falta de documentación
	Configuración incorrecta de parámetros del software
	Fechas incorrectas del software
	Mecanismos de identificación y autenticación insuficientes
	Tablas de contraseñas desprotegidas
	Mala gestión en la fortaleza de las contraseñas
	Funcionalidades del software innecesarios habilitados
	Software inmaduro o nuevo
	Especificaciones poco claras o incompletas para los desarrolladores
	Control de cambios ineficaz
	Descarga y uso incontrolado del software
	Copias de seguridad incompletas o inexistentes
Red	Gabinetes de red desprotegidos
	Cableado de red desprotegido
	Tráfico confidencial sin protección
	Mecanismos ineficaces o inexistentes de identificación y autenticación en la red
	Arquitectura de red insegura
	Transferencia de contraseñas en texto plano
	Configuración de los equipos de red inadecuadas
	Conexiones de red pública sin protección
Personal	Ausencia de personal
	Procedimientos de contratación inadecuados
	Insuficiente formación en seguridad de la información

	Uso incorrecto del software y hardware
	Poca conciencia de seguridad de la información
	Trabajo no supervisado por personal externo o de limpieza
	Políticas ineficaces o inexistentes para el correcto uso de los servicios de red y de los sistemas
Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones
	Ubicación en una zona susceptible a inundaciones
	Ubicación en una zona susceptible a incendios
	Red eléctrica inestable
	Protección física insuficiente del edificio, puertas y ventanas
Organización	Procedimiento formal para el alta y baja de usuarios no desarrollado, o su implementación es inefectiva
	Disposiciones insuficientes (sobre seguridad) en contratos
	Procedimiento de monitoreo de instalaciones de procesamiento de información no desarrollado, o su implementación es ineficaz.
	Auditorías no realizadas periódicamente
	Procedimientos de identificación y evaluación de riesgos no desarrollados, o su implementación es ineficaz
	Informes de fallos insuficientes o inexistentes registrados en los registros del administrador y del operador
	Inadecuada respuesta de mantenimiento del servicio
	Acuerdo de nivel de servicio insuficiente o inexistente
	Procedimiento de control de cambios no desarrollado, o su implementación es ineficaz
	No se ha desarrollado un procedimiento formal para el control de la documentación del SGSI o su implementación es ineficaz
	No se ha desarrollado un procedimiento formal para la supervisión de registros del SGSI o su implementación es ineficaz
	Proceso formal para la autorización de la información institucional no desarrollado, o su implementación es inefectiva
	Asignación inadecuada de responsabilidades de seguridad de la información
	Los planes de continuidad no existen, o está incompletos, o están desactualizados
	Política de uso de correo electrónico no desarrollada, o su implementación es ineficaz
	Procedimientos para el manejo de información clasificada no desarrollados, o su implementación es inefectiva
	Las responsabilidades de seguridad de la información no están presentes en las descripciones de los puestos
	Disposiciones insuficientes o inexistentes (relativas a la seguridad de la información) en los contratos con los empleados
	Proceso disciplinario en caso de incidente o evento de seguridad no definido, o no funcione correctamente
	No se ha desarrollado una política formal sobre el uso de computadoras móviles o su implementación es ineficaz
	Control insuficiente de los activos fuera de las instalaciones
	Política insuficiente o inexistente de “escritorio y pantalla limpia”
	Autorización de ingreso a las instalaciones de procesamiento de información no implementada o no funciona correctamente
	Mecanismos de monitoreo de brechas de seguridad no implementados adecuadamente
	Procedimientos para reportar debilidades de seguridad no desarrollados, o su implementación es ineficaz

	Procedimientos de cumplimiento de disposiciones sobre derechos intelectuales no desarrollados, o su implementación es ineficaz
	No se ha desarrollado una política formal sobre el uso de la nube o su implementación es ineficaz

FUENTE: Norma ISO 27005

- Descripción del Riesgo: Denominación que se le brinda al riesgo identificado considerando redactarlo como la conjugación de AMENAZA + VULNERABILIDAD en relación con los campos previamente identificados.
- Propietario del Riesgo: Se registra el órgano o unidad orgánica responsable de la gestión, seguimiento y control del riesgo asignado. Debe asegurar el cumplimiento del tratamiento del riesgo.
- Pilar de Seguridad de la Información afectado: Se marca con una "X" dependiendo del pilar de seguridad de la información afectado: Confidencialidad, integridad o disponibilidad.

5.3.3 ANÁLISIS Y VALORACIÓN DEL RIESGO

Para el análisis y valoración del riesgo, el Órgano dueño del proceso y su equipo, en coordinación con el Oficial de Seguridad y Confianza Digital, continuando con el resultado del párrafo anterior, se realiza la "Evaluación de Control Existente", el cual debe ser evaluado bajo los criterios establecidos. Posterior al resultado de la evaluación de control existente, se registra el código y la descripción del control actual. Se registra en el formato (Ver Anexo N° 5: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (Hoja SIN_IAV)), realizando los siguientes pasos:

- Paso 1: Valoran la probabilidad de la materialización del riesgo inherente, considerando los niveles de posibilidad que el evento de riesgo ocurra, de acuerdo a la siguiente tabla:

TABLA N° 19: NIVELES DE PROBABILIDAD

Probabilidad	Valor	Descripción
MUY ALTA	10	El riesgo podría ocurrir en la mayoría de las circunstancias en un presente muy cercano o aproximadamente en días o semanas.
ALTA	8	El riesgo puede ocurrir en la mayoría de las circunstancias o aproximadamente una vez al mes.
MEDIA	6	El riesgo puede ocurrir en algún momento relativamente frecuente o en un futuro cercano menor a un semestre.
BAJA	4	El riesgo podría ocurrir rara vez sólo en circunstancias excepcionales o en un horizonte aproximado mayor a un año.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

- Paso 2: Valoran el impacto de la materialización del riesgo inherente, considerando los valores de la siguiente tabla (Ver Anexo N° 5: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (Hoja SIN_IAV))

TABLA N° 20: NIVELES DE IMPACTO		
Impacto negativo	**Valor**	**Descripción**
Muy Alto	**10**	Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo la confidencialidad, integridad y disponibilidad de información crítica del RENIEC o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio.
Alto	**8**	Si el evento llegara a presentarse, tendría un alto impacto comprometiendo la confidencialidad y/o integridad y/o disponibilidad de información crítica del RENIEC o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio (se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves del RENIEC por un tiempo considerable).
Medio	**6**	Si el evento llegara a presentarse, tendría un moderado impacto sobre la confidencialidad o integridad o disponibilidad de la información. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
Bajo	4	Si el evento llegara a presentarse, no representa un impacto importante para el RENIEC.

FUENTE: Elaboración del Oficial de Seguridad y Confianza Digital

- Paso 3: Calculan el nivel de exposición del riesgo inherente, producto de la probabilidad e impacto obtenidos.
- Paso 4: Registran la información de los controles existentes vinculados al proceso analizado.
- Paso 5: Utilizan el resultado de la efectividad del o de los controles existentes, como insumos para la valoración de la probabilidad e impacto del riesgo después de los controles existentes, con el cual obtienen el nivel de exposición del riesgo residual, es decir, antes del tratamiento.
- Paso 6: Comparar el nivel de exposición obtenido con el nivel de tolerancia establecido por la Entidad. Si el nivel de exposición es bajo el riesgo puede ser aceptado, en el caso de los demás niveles (medio, alto o muy alto) el riesgo debe pasar a tratamiento.
- Paso 7: Seleccionar el nivel de prioridad, se determina e función al nivel de riesgo considerándose como Prioridad 1, al nivel del riesgo “MUY ALTO”; Prioridad 2, al nivel de riesgo “ALTO”; y Prioridad 3, al nivel de riesgo “MEDIO”.
- Paso 8: El dueño del proceso, el gestor líder y equipo de riesgos revisan y validan el análisis y la valoración de los riesgos identificados.

5.3.4 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo implica identificar, evaluar y mitigar las vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información. Este proceso se lleva a cabo mediante la implementación de controles y medidas de control diseñados para reducir el impacto de los riesgos identificados, asegurando así la protección de los activos de información de la Entidad. Para el tratamiento del riesgo, el “**Órgano dueño del proceso**” y su equipo, en coordinación del Oficial de Seguridad y Confianza Digital Para ello, registra en el formato correspondiente (Ver Anexo N° 6: PLAN DE GESTIÓN INTEGRAL DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN – TRATAMIENTO (hoja SIN_TR)), se debe seguir los siguientes pasos:

- Paso 1: Identificar los riesgos a tratar, considerando criterios para la gestión integral del riesgo.
- Paso 2: Establecer y redactar los controles (orientados a mitigar las amenazas y/o vulnerabilidades identificadas), así como la fecha de implementación, los medios de verificación y órganos responsables de su ejecución.
- Paso 3: Establecer y redactar las acciones para cada una de los controles, teniendo como referencia los controles de la norma ISO 27001. Registrar la fecha de implementación, los medios de verificación y órganos responsables de su ejecución. (Ver TABLA N° 21: CONTROLES DE REFERENCIA DEL ANEXO A DE LA ISO 27001).
- Paso 4: Revisar y validar el tratamiento otorgado a cada uno de los riesgos identificados con la finalidad de derivarlos al Oficial de Seguridad y Confianza Digital para su revisión correspondiente
- Paso 5: El Oficial de Seguridad y Confianza Digital evalúa y valida la pertinencia y factibilidad del control o controles y acciones definidas en los Planes de Gestión Integral del Riesgo y los Planes de Acción Anual Medidas de Control.

5.3.5 REMISIÓN Y APROBACION DEL PGIR/PAAMC

La aprobación del plan de riesgos, implica la ratificación formal de un documento que detalla los riesgos identificados y las estrategias para mitigarlos. Para ello, se debe seguir los siguientes pasos:

- Paso 1: El dueño del proceso, revisa y aprueba el PGIR/PAAMC del proceso a su cargo, con la finalidad de remitirlo al Oficial de Seguridad y Confianza Digital para su revisión
- Paso 2: El Oficial de Seguridad y Confianza Digital revisa y realiza la retroalimentación correspondiente al órgano dueño del proceso para los ajustes pertinentes
- Paso 3: El dueño del proceso remite la versión aprobada y firmada del PGIR/PAAMC al Oficial de Seguridad y Confianza Digital y a la a OILCC.

5.3.6 SEGUIMIENTO DE LAS ACCIONES PLANIFICADAS PARA EL TRATAMIENTO DE RIESGOS

La ejecución comprende la implementación de las acciones y medidas de control o controles consignadas en el PGIR/PAAMC, orientadas a la reducción o mitigación de los riesgos que se encuentran en la etapa de tratamiento. Esta actividad es desarrollada por los órganos dueños del proceso y reportada de manera mensual al Oficial de Seguridad y Confianza Digital y a la a OILCC, adjuntando las evidencias que corroboren el avance progresivo.

El seguimiento se encuentra a cargo del al Oficial de Seguridad y Confianza Digital y su equipo, quien monitorea de manera mensual la ejecución de las acciones y medidas de control consideradas en el PGIR/PAAMC, el seguimiento permite determinar el estado de ejecución de cada una de las

acciones y controles consignados, sobre la base de la información y documentación que es proporcionada por los órganos dueños del proceso. El estado de ejecución de las medidas de control se determina considerando los siguientes criterios:

TABLA N° 12: ESTADO DE LA MEDIDA DE CONTROL

Estado	Criterio
Implementada	Cuando el responsable ha cumplido con implementar la medida de control conforme al PGIR/PAAMC.
No implementada	Cuando el responsable no ha cumplido con implementar la medida de control contenida en el PGIR/PAAMC y el plazo para su ejecución ha culminado definitivamente.
En proceso	Cuando el responsable ha iniciado, pero aún no ha culminado con la implementación de la medida de control contenida en el PGIR/PAAMC
Pendiente	Cuando el responsable no ha iniciado la implementación de la medida de control contenida en el PGIR/PAAMC.
No aplicable	Cuando la medida de control contenida en el PGIR/PAAMC, no puede ser ejecutada por factores no atribuibles al dueño del proceso, debidamente sustentados, que imposibilitan su implementación.
Desestimada	Cuando el responsable decide no implementar la medida de control contenida en el PGIR/PAAMC, asumiendo las consecuencias de dicha decisión.

FUENTE: Elaboración OILCC

Para realizar el seguimiento de las acciones asociadas a cada medida de control establecida para el tratamiento de los riesgos de seguridad de la información se debe realizar los siguientes pasos:

- Paso 1: El Gestor Líder y equipo de riesgos/gestores operativos ejecutan las acciones asociadas a cada control o medida de control vinculada a los riesgos de seguridad de la información identificados. Registran el avance mensual y adjuntan las evidencias que corresponden.
- Paso 2: El órgano dueño del proceso traslada el avance de ejecución al Oficial de Seguridad y Confianza Digital con conocimiento de la OILCC.
- Paso 3: El Oficial de Seguridad y Confianza Digital junto a su equipo de trabajo revisa y valida el avance reportado por el órgano dueño del proceso, conforme a los medios de verificación (evidencias) remitidos. Comunica el resultado a los dueños de proceso y a la OILCC.
- Paso 4: La OILCC consolida la información remitida por el Oficial de Seguridad y Confianza Digital e incorpora los avances obtenidos en el informe de resultado mensual que remite a la Secretaría General y Gerencia General con la finalidad que tomen conocimiento de los avances obtenidos por los órganos dueños de los procesos.
- Paso 5: La Secretaría General o Gerencia General, según corresponda, toman conocimiento de lo expuesto en el informe de resultado remitido por la OILCC.

5.3.7 IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN Y TRATAMIENTO DE OPORTUNIDADES

Las oportunidades son situaciones favorables que podrían permitir el logro de los objetivos, una desviación positiva que surge de un riesgo puede proporcionar una oportunidad. Se considera que "riesgos" y "oportunidades" deben ser gestionados, ya que el enfoque dado es "hacer las cosas bien", teniendo en cuenta la situación actual (y sus riesgos), así como mejorar de cara a futuro (teniendo en cuenta las oportunidades). Por ejemplo, un conjunto de circunstancias que permita a la Entidad, desarrollar nuevos productos y servicios, optimización de los procesos, reducir las mermas o mejorar la productividad de los productos y servicios.

Para el tratamiento de las oportunidades se debe priorizar aquellas que luego de ser evaluadas se encuentren en los niveles de exposición **"Alto"** y **"Muy Alto**". Asimismo, se debe considerar los riesgos asociados.
Para identificar, analizar, valorar y tratar las oportunidades se debe utilizar el Registro N° 6: Plan de Gestión de Oportunidades del Anexo N° 06 y las tablas contenidas en el Anexo N° 07.

5.4 RIESGO QUE AFECTAN LA INTEGRIDAD PÚBLICA

Para la gestión de este tipo de riesgos, la Entidad ha adoptado la metodología establecida en la "Guía para la gestión de riesgos que afectan la Integridad Pública", la misma que fue aprobada por Resolución 001-2023-PC/SIP de la Secretaría de Integridad Pública de la Presidencia del Consejo de Ministros.

En ese sentido, el riesgo que afecta la integridad pública o riesgo de Integridad se definen como la posibilidad 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. Es posible distinguir diversas prácticas, según su gravedad y consecuencia tales como:

a) 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.

b) 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.

c) Riesgo de práctica cuestionable

Posibilidad de que ocurra un comportamiento, por acción u omisión, que transgreda los principios éticos y los valores de la organización. En caso de materializarse el riesgo, no llegaría a ser sancionable en el ámbito administrativo.

En ese sentido, se han definido tres tipos de riesgos que afectan la integridad pública. Sin embargo, la metodología de gestión de riesgos que afecta la integridad pública se enfoca en la gestión de los riesgos de corrupción e inconducta funcional, ya que las prácticas cuestionables serán abordadas como parte del tratamiento vinculado a las posibles causas de alguno de los otros dos tipos de riesgo. Debido que dichas prácticas suelen tener su origen en situaciones normalizadas o al deterioro del carácter ético de algunos servidores públicos. Por ello, es importante efectuar un trabajo de promoción transversal de principios y valores organizacionales. Para la presente metodología se han establecido roles, los cuales han sido difundidos por la Secretaría General y son:

- Rol de Alta dirección
- Rol conductor
- Rol técnico
- Rol consultivo

5.4.1 IDENTIFICACIÓN DE RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA

Se realiza en dos niveles. El primer nivel está a cargo de los servidores de los órganos y unidades orgánicas con rol técnico (dueños del proceso, gestor líder junto al equipo de riesgos/gestores operativos); el segundo, a cargo del rol conductor (órgano que ejerce la función de integridad - OILCC), con la asistencia de los órganos que ejercen el rol consultivo (Secretaria Técnica de Procedimientos Administrativos Disciplinarios, Procuraduría Publica y la Oficina de Planificación, Presupuesto y Modernización) que hayan sido convocados. Ambos niveles son registrados en el formato Excel (ver Anexo N° 7: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA (hoja INT_IAV), que genera de manera automática el formato “Ficha N° 1: Identificación de riesgo que afecta la Integridad Pública”. (ver Anexo N° 11: FICHAS PARA LA GESTION DE RIESGOS QUE AFECTAN LA INTEGRIDAD PUBLICA (PCM/SIP), (hoja Fichas).

Primer nivel de identificación

En el presente nivel el gestor líder junto al equipo de riesgos/gestores operativos realizan los siguientes pasos:

- Paso 1: Determinar la ubicación del riesgo en el proceso en el cual se encuentra involucrado (proceso operativo, misional o proceso de soporte)
- Paso 2: Identificar los contextos de riesgo que involucran principalmente relaciones de la entidad con actores externos (por ejemplo, en las contrataciones y en la prestación directa de servicios al usuario) y

relaciones entre actores internos de la entidad (gestión de personal o gestión de dinero entregado a servidores de la entidad).

- Paso 3: Identificar posibles comportamientos irregulares asociados a prácticas que afectan la integridad pública.
- Paso 4: Identificar potenciales agentes de riesgo (agente primario, agente interno y agente externo).
- Paso 5: Formular o redactar el riesgo, considerando la siguiente estructura: [Agente potencial + Verbo en condicional simple (Podría) + Posible comportamiento irregular, en el Contexto en el que se produce el riesgo]. Por ejemplo: "El registrador civil de trámite de DNI podría solicitar un soborno a los usuarios para realizar un registro civil con información falsa, durante el proceso del registro civil"

Segundo nivel de identificación

En el presente nivel el gestor líder junto al equipo de riesgos/gestores operativos realizan los siguientes pasos:

- Paso 6: Establecer si se trata de un riesgo de corrupción o de inconducta funcional, se debe validar si se cumple alguna de las condiciones indicadas. Para ambos tipos de riesgo, debe validarse el incumplimiento explícito de una norma o disposición legal. En el caso del riesgo de inconducta funcional, debe validarse el ejercicio inadecuado de la función.
- Paso 7: Remitir la ficha que contiene el riesgo identificado al responsable del rol conductor (OILCC), con la finalidad de validar el riesgo registrado y determinar junto al rol consultivo el tipo de riesgo identificado (corrupción y/o inconducta funcional).
- Paso 8: La OILCC, en el rol conductor, junto a la USTPAD, PPU y OPPM, en el rol consultivo, devuelve la ficha que contiene el riesgo validado al órgano dueño del proceso para que continúen con la siguiente etapa.

5.4.2 EVALUACIÓN DE RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA

La evaluación es un proceso que permite analizar y valorar los riesgos, durante esta etapa, los servidores con rol técnico determinan las causas del riesgo (hasta tres causas, numeradas en orden de prioridad) y sus efectos correspondientes (estableciendo una jerarquía en términos de importancia). Asimismo, estiman su probabilidad e impacto, considerando la regla de decisión establecida en la Guía de gestión de riesgos que afectan la integridad pública. Esta actividad se registra en el formato Excel (ver Anexo N° 7: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA (hoja INT_IAV), que genera de manera automática el formato "Ficha N° 2: Evaluación del riesgo que afecta la integridad pública". (ver Anexo N° 11: FICHAS PARA LA GESTION DE RIESGOS QUE AFECTAN LA INTEGRIDAD PUBLICA (PCM/SIP), (hoja Fichas).

El órgano que ejerce la función de integridad valida la evaluación efectuada por los servidores con rol técnico y, de ser el caso, convoca a los servidores

con rol consultivo que corresponda, según sus competencias y experiencia, para contar con elementos de análisis que permitan dicha validación. Para ello, el gestor líder junto al equipo de riesgos/gestores operativos realizan los siguientes pasos:

- Paso 1: Identificar las causas personales y organizacionales que podrían generar la materialización del riesgo y sus posibles efectos, más allá de las consecuencias administrativas, civiles o penales para los agentes involucrados.
- Paso 2: Valorar el nivel de probabilidad e impacto del riesgo analizado, considerando la regla de decisión establecida en la Guía de gestión de riesgos que afectan la integridad pública.
- Paso 3: Realizar el cálculo del nivel de exposición del riesgo residual, el mismo que es el producto de la probabilidad e impacto.
- Paso 4: Seleccionar la opción de tratamiento al riesgo de acuerdo al nivel de tolerancia establecido en la política de gestión de riesgos de la Entidad.
- Paso 5: El gestor líder junto al dueño del proceso revisan el registro que incluye los riesgos identificados en el proceso.
- Paso 6: Remitir la ficha que contiene el riesgo identificado al responsable del rol conductor (OILCC), con la finalidad de validar evaluación efectuada y, de ser el caso, convoca a los servidores con rol consultivo que corresponda, según sus competencias y experiencia, para contar con elementos de análisis que permitan dicha validación.
- Paso 7: La OILCC, en el rol conductor, junto a la USTPAD y PPU, en el rol consultivo, en caso corresponda, devuelven la ficha que contiene el riesgo validado al órgano dueño del proceso para que continúen con la siguiente etapa.

5.4.3 TRATAMIENTO DE RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA

En esta etapa se determinan las medidas de prevención o mitigación de riesgos que serán aplicada a los riesgos identificados, las cuales serán registradas en el plan de acción correspondiente. La implementación de estas medidas se encuentra a cargo de los dueños de proceso y unidades orgánicas responsables de los procesos donde se identificaron los riesgos.

Los servidores con rol técnico proponen las medidas de prevención o mitigación. Posteriormente, comunican la propuesta al responsable del órgano que ejerce la función de integridad, quien valida la pertinencia y factibilidad de las medidas propuestas y, de ser el caso, convoca a los servidores con rol consultivo que corresponda, según sus competencias y experiencia, para contar con elementos de análisis que permitan dicha evaluación.

Esta actividad se registra en el formato Excel, (ver Anexo N° 7: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA (hoja INT_IAV), que genera de manera automática el

formato “Ficha N° 3: Tratamiento del riesgo que afecta la integridad pública”. (ver Anexo N° 11: FICHAS PARA LA GESTION DE RIESGOS QUE AFECTAN LA INTEGRIDAD PUBLICA (PCM/SIP), (hoja Fichas). Para ello, el gestor líder junto al equipo de riesgos/gestores operativos realizan los siguientes pasos:

- Paso 1: Proponer medidas de prevención, orientadas a reducir las causas del riesgo identificado o medidas de mitigación, orientadas a mitigar los efectos y mejorar la capacidad de respuesta de la entidad, en caso de materialización del riesgo.
- Paso 2: Establecer las estrategias y medidas de prevención o mitigación, las cuales se registran como medidas de control, incluyendo además la fecha de inicio y término de su implementación, los medios de verificación resultantes y órganos responsables de su ejecución, las mismas que son registradas en el formato Excel, (ver Anexo N° 8: PLAN DE GESTIÓN INTEGRAL DEL RIESGO QUE AFECTA LA INTEGRIDAD PÚBLICA – TRATAMIENTO (hoja INT_TR)).
- Paso 3: Revisar y validar junto al dueño del proceso el tratamiento otorgado a cada uno de los riesgos identificados.
- Paso 4: Remitir la ficha que contiene el riesgo identificado al responsable del rol conductor (OILCC), con la finalidad de validar las medidas de prevención o mitigación establecidas para el tratamiento del riesgo (medidas de control, acciones, medios de verificación, responsables y plazos de ejecución), quien, de ser el caso, convoca a los servidores con rol consultivo que corresponda, según sus competencias y experiencia, para contar con elementos de análisis que permitan dicha validación.
- Paso 5: La OILCC, en el rol conductor, junto a la USTPAD, PPU y OPPM, en el rol consultivo, en caso corresponda, devuelven la ficha que contiene las medidas de prevención o mitigación y medidas de control validadas, consideradas para el tratamiento del riesgo al órgano dueño del proceso.
- Paso 6: El órgano dueño del proceso firma de manera digital las fichas 1, 2 y 3 (ver Anexo N° 11: FICHAS PARA LA GESTION DE RIESGOS QUE AFECTAN LA INTEGRIDAD PUBLICA (PCM/SIP), (hoja Fichas)) que contienen el análisis, valoración y tratamiento del riesgo que afecta la integridad pública al responsable del rol conductor (OILCC) para su consolidación y gestión de la aprobación correspondiente a través del Plan de Gestión Integral del Riesgo (PGIR) o Plan de Acción Anual Medidas de Control (PAAMC), según corresponda.

5.4.4 SEGUIMIENTO Y MEJORA CONTINUA

5.4.4.1 Seguimiento a la ejecución de las medidas de control

La ejecución comprende la implementación de las acciones y medidas de control consignadas en el PGIR/PAAMC, orientadas a la reducción o mitigación de los riesgos que se encuentran en la etapa de tratamiento. Esta actividad es desarrollada por los órganos dueños del proceso y reportada de manera mensual a la OILCC,

adjuntando las evidencias (medios de verificación) que corroboren el avance progresivo.

El seguimiento se encuentra a cargo del responsable de la función de cumplimiento/antisoborno (OILCC), quien monitorea de manera mensual la ejecución de las acciones y medidas de control consideradas en el PGIR/PAAMC. El seguimiento permite determinar el estado de ejecución de cada una de las acciones y medidas de control consignadas, sobre la base de la información y documentación que proporcionada por los órganos dueños del proceso. El estado de ejecución de las medidas de control se determina considerando los siguientes criterios:

TABLA N° 12: ESTADO DE LA MEDIDA DE CONTROL

Estado	Criterio
Implementada	Cuando el responsable ha cumplido con implementar la medida de control conforme al PGIR/PAAMC.
No implementada	Cuando el responsable no ha cumplido con implementar la medida de control contenida en el PGIR/PAAMC y el plazo para su ejecución ha culminado definitivamente.
En proceso	Cuando el responsable ha iniciado, pero aún no ha culminado con la implementación de la medida de control contenida en el PGIR/PAAMC
Pendiente	Cuando el responsable no ha iniciado la implementación de la medida de control contenida en el PGIR/PAAMC.
No aplicable	Cuando la medida de control contenida en el PGIR/PAAMC, no puede ser ejecutada por factores no atribuibles al dueño del proceso, debidamente sustentados, que imposibilitan su implementación.
Desestimada	Cuando el responsable decide no implementar la medida de control contenida en el PGIR/PAAMC, asumiendo las consecuencias de dicha decisión.

FUENTE: Elaboración OILCC

En ese sentido, el Gestor Líder junto al equipo de riesgos/gestores operativos, debe emplear el registro en formato Excel, ver (Anexo N° 8: PLAN DE GESTIÓN INTEGRAL DEL RIESGO QUE AFECTA LA INTEGRIDAD PÚBLICA – TRATAMIENTO (hoja INT_TR)) y seguir los siguientes pasos:

- Paso 1: Ejecutar las acciones asociadas a cada medida de control vinculada a los riesgos que afectan la integridad pública identificados en su proceso, registrando el avance mensual y adjuntando las evidencias que corresponden.
- Paso 2: Trasladar el avance de ejecución al responsable de la función de cumplimiento/antisoborno (OILCC).
- Paso 3: El responsable de la función de cumplimiento/antisoborno (OILCC) junto a su equipo de trabajo

revisa y valida el avance reportado por el órgano dueño del proceso, conforme a los medios de verificación remitidos.

- Paso 4: La OILCC incorpora los avances obtenidos en el informe de resultado mensual que remite a la Secretaría General y Gerencia General con la finalidad que tomen conocimiento de los avances obtenidos por los órganos dueños de los procesos.
- Paso 5: La OILCC comunica a los órganos dueños de los procesos, mediante correo electrónico, los avances y comentarios consignados.
- Paso 6: La Secretaría General o Gerencia General, según corresponda, toman conocimiento de lo expuesto en el informe de resultado remitido por la OILCC y disponen la adopción de las acciones correspondientes.

5.4.4.2 Mejora Continua

Uso de la información de gestión de riesgos para la mejora continua, cuando la entidad gestiona los riesgos que afectan la integridad pública se genera información importante:

- El inventario de riesgos, en la etapa de identificación
- El mapa de riesgos, en la etapa de evaluación
- El plan de acción anual, en la etapa de tratamiento
- Los reportes de seguimiento del plan, en la etapa de seguimiento y mejora continua.

5.4.5 REMISIÓN Y APROBACION DEL PGIR/PAAMC

La aprobación del plan de riesgos, implica la ratificación formal de un documento que detalla los riesgos identificados y las estrategias para mitigarlos. Para ello, se debe seguir los siguientes pasos:

- Paso 1: El dueño del proceso, revisa y aprueba el PGIR/PAAMC del proceso a su cargo, con la finalidad de remitirlo al responsable de la función de Cumplimiento/Antisoborno para su revisión
- Paso 2: El responsable de la función de Cumplimiento/Antisoborno revisa y realiza la retroalimentación correspondiente al órgano dueño del proceso para los ajustes pertinentes
- Paso 3: El dueño del proceso remite la versión aprobada y firmada del PGIR/PAAMC a la OILCC para su consolidación y registro (PAAMC) en el aplicativo informático del SCI de la CGR.
- Paso 4: La OILCC gestiona el visado del PGIR/PAAMC a través de la Secretaría General o Gerencia General, según corresponda. Además de la aprobación y envío a la Contraloría General de la República por parte de la Jefatura Nacional (solo en el caso del PAAMC).

VI. ANEXOS

Los anexos para la aplicación metodológica de la gestión integral del riesgo y oportunidades (PGIR/PAAMC/PGO) para las etapas de identificación, análisis, valoración, tratamiento, seguimiento, reevaluación y efectividad de controles, son gestionados con el uso de una herramienta elaborada en Microsoft Excel, la misma que se encuentra disponible en el micrositio de la OILCC, a través del siguiente enlace:

https://identidad.reniec.gob.pe/integridad-y-calidad

6.1 Anexo N° 1: EVALUACIÓN DE CONTROLES EXISTENTES / IMPLEMENTADOS.

6.2 Anexo N° 2: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS OPERATIVOS.

6.3 Anexo N° 3: PLAN DE GESTIÓN INTEGRAL DEL RIESGO OPERATIVO – TRATAMIENTO.

6.4 Anexo N° 4: INVENTARIO DE ACTIVOS DE INFORMACIÓN.

6.5 Anexo N° 5: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

6.6 Anexo N° 6: PLAN DE GESTIÓN INTEGRAL DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN – TRATAMIENTO.

6.7 Anexo N° 7: PLAN DE GESTIÓN INTEGRAL DEL RIESGO - RIESGOS QUE AFECTAN LA INTEGRIDAD PÚBLICA.

6.8 Anexo N° 8: PLAN DE GESTIÓN INTEGRAL DEL RIESGO QUE AFECTA LA INTEGRIDAD PÚBLICA – TRATAMIENTO.

6.9 Anexo N° 9: REGISTRO PARA IDENTIFICACION DE RIESGOS EN NUEVOS PRODUCTOS, SERVICIOS O INICIATIVAS.

6.10 Anexo N° 10: REPORTE DE SITUACIONES ADVERSAS (RIESGO MATERIALIZADO).

6.11 Anexo N° 11: FICHAS PARA LA GESTION DE RIESGOS QUE AFECTAN LA INTEGRIDAD PUBLICA (PCM/SIP).