RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

MANUAL

GESTIÓN INTEGRAL DEL RIESGO

RESOLUCIÓN SECRETARIAL N° 34 -2019-SGEN/RENIEC		
MGIR-200-GG/OFCR/001	VERSIÓN: 01	FECHA DE APROBACIÓN
	N° PÁGINAS: 62	08 ABR. 2019

ÍNDICE

I. OBJETIVO

Establecer la metodología y estandarización para la implementación y sostenibilidad a la Gestión Integral del Riesgo, aplicada en la gestión institucional, brindándonos una seguridad razonable en el logro de los objetivos institucionales y el cumplimiento de las disposiciones legales y normativas del Estado.

II. ALCANCE

El presente manual es administrado por la Gerencia General (GG), a través de la Oficina de Fiscalización, Control y Riesgos (OFCR); siendo de aplicación obligatoria en los procesos, procedimientos y actividades en todos los órganos y en los diferentes niveles de la institución.

III. REFERENCIAS NORMATIVAS

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

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

3.3 **Ley N° 28716,** Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006.

3.4 **Ley N° 29664,** crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), del 19 febrero de 2011 y modificatorias.

3.5 **Decreto Supremo N° 015-98-PCM,** aprueba el Reglamento de las Inscripciones del Registro Nacional de Identificación y Estado Civil, del 25 de abril de 1998 y modificatorias.

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

3.7 **Decreto Supremo N° 051-2010-MTC**, aprueba el "Marco Normativo General del Sistema de Comunicaciones en Emergencias", modifica el Plan Técnico Fundamental de Numeración, aprobado por R.S. N° 022-2002-MTC, el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por D.S. N° 020-2007-MTC y el Reglamento de la Ley de Radio y Televisión, aprobado por D.S. N° 0052005-MTC; y deroga los DD.SS. N° 0302007-MTC y N° 043-2007-MTC, del 19 octubre de 2010.

3.8 **Decreto Supremo N° 048-2011-PCM,** aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), del 26 mayo de 2011.

3.9 **Decreto Supremo N° 111-2012-PCM,** incorpora la Política Nacional de Gestión del Riesgo de Desastres como Política Nacional de obligatorio cumplimiento para las entidades del Gobierno Nacional, del 2 noviembre de 2012.

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

3.11 **Decreto Supremo N° 034-2014-PCM,** dispone la aprobación del Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2014-2021, del 13 mayo de 2014.

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

3.13 **Decreto Supremo N° 044-2018-PCM,** aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021, del 26 abril de 2018.

3.14 **Decreto Supremo N° 050-2018-PCM,** aprueba la Seguridad Digital en el Ámbito Nacional, del 15 mayo de 2018.

3.15 Decreto Supremo N° 004-2019-JUS, aprueba Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, del 25 de enero de 2019.

3.16 Resolución Ministerial N° 046-2013-PCM, aprueba la Directiva "Lineamientos que definen el Marco de Responsabilidades en Gestión del Riesgo de Desastres, de las entidades del estado en los tres niveles de gobierno" y su anexo, del 15 febrero de 2013.

3.17 Resolución Ministerial N° 028-2015-PCM, aprueban Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno, del 7 febrero de 2015.

3.18 Resolución Ministerial N° 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, del 16 de enero de 2016 y su modificatoria.

3.19 Resolución Ministerial N° 166-2017-PCM, modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información, del 21 de junio de 2017.

3.20 Resolución de Contraloría N° 320-2006-CG, aprueban Normas de Control Interno, del 3 de noviembre de 2006.

3.21 Resolución de Contraloría N° 004-2017-CG, aprueba la "Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado", del 20 de enero de 2017

3.22 Resolución Directoral N° 014-2018-INACAL/DN, aprueba la Norma Técnica Peruana NTP-ISO 31000:2018 Gestión del Riesgo. Directrices, 2ª Edición, del 4 de julio de 2018.

3.23 Resolución Jefatural N.° 073-2016-JNAC/RENIEC, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 1 de junio de 2016 y modificatoria.

3.24 Resolución Jefatural N° 135-2017/JNAC/RENIEC, aprueba la Política y Objetivos de la Gestión Integral del Riesgo, del 23 de octubre de 2017.

3.25 Resolución Jefatural N° 124-2018/JNAC/RENIEC, aprueba el Plan Estratégico Institucional 2018-2020 del RENIEC, del 24 octubre de 2018.

3.26 Resolución Jefatural N° 021-2019/JNAC/RENIEC, faculta a la Secretaría General, la aprobación de documentos normativos del RENIEC, del 11 de febrero de 2019.

3.27 Resolución Secretarial N° 055-2017/SGEN/RENIEC, aprueba la Directiva DI-200-GPP/001 sobre "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", del 28 de agosto de 2017 y modificatoria.

3.28 Resolución Secretarial N° 032-2018/SGEN/RENIEC, aprueba la Directiva DI-418-GG/OFCR/002 "Gestión Integral del Riesgo", primera versión, del 18 de abril de 2017.

3.29 Norma Internacional EN 31010:2010, adopta la Norma Internacional ISO/IEC 31010:2009. "Gestión del riesgo - Técnicas de apreciación del riesgo".

3.30 COSO ERM Integrating with Strategy and Performance, del 19 junio 2017.

IV. DEFINICIÓN DE TÉRMINOS

4.1 Apetito por el Riesgo
Cantidad y tipo de riesgo que una organización está preparada para buscar o retener.

4.2 Amenaza
Causa potencial de un incidente no deseado, el cual puede causar el daño a uno o varios activos de información.

4.3 Confidencialidad
Propiedad de la información que pretende garantizar el acceso solo a las personas autorizadas.

4.4 Contexto Externo
Entorno externo en el que la organización busca alcanzar sus objetivos.

4.5 Contexto Interno
Entorno interno en el que la organización busca alcanzar sus objetivos.

4.6 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.

4.7 Control Existente
Medida que actualmente está en vigencia y modifica el riesgo siendo identificado en la etapa de Análisis y valoración del Riesgo.

4.8 Control Implementado
Es aquel control que se desarrolla para modificar un riesgo y que se establece en la etapa de Tratamiento del Riesgo.

4.9 Coordinador del riesgo
Responsable designado por el Órgano correspondiente, quien realizará las coordinaciones con la OFCR, sobre la Gestión del Riesgo en sus procesos. En riesgos de Seguridad de la Información ese rol es equivalente al del Gestor Líder de Seguridad de la Información.

4.10 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.

4.11 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 y otros requisitos que se deben cumplir.

4.12 Disponibilidad
Propiedad de la información de estar disponible y utilizable cuando lo requiera una entidad autorizada.

4.13 Evento
Ocurrencia o cambio de un conjunto particular de circunstancias. En seguridad de la información está referida a una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación a la política de seguridad de la información, o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la información.

4.14 Equipo de Riesgos
Equipo técnico multifuncional, designado por los Gestores del Riesgo, es equivalente al Equipo de Riesgos de Seguridad de la Información.

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

4.16 Gestión Integral del Riesgo
Aplicación sistemática de políticas, procedimientos y prácticas de gestión que brindan una seguridad razonable para el cumplimiento de los objetivos institucionales. Se implanta como un sistema de gestión que constituye una herramienta que permite integrar otros sistemas de gestión reconocidos, como el de gestión de la calidad ISO 9001, gestión ambiental ISO 14001, gestión de seguridad y salud en el trabajo ISO 45001, seguridad de la información ISO 27001 o cualquier otro sistema de gestión basado en el ciclo PDCA y la mejora continua.

4.17 Gestor del Riesgo
Dueño del proceso o Gerente designado que gestiona el proceso; con responsabilidad y autoridad para gestionar el riesgo, rol equivalente al Dueño del Riesgo para riesgos en Seguridad de la Información.

4.18 Gobierno Digital
El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

4.19 Impacto o Consecuencias
Resultado de un evento o incidente que afecta a los objetivos. Es el daño sobre el activo derivado de la materialización de la amenaza.

4.20 Incidente
Situación que da o podría dar lugar, a una interrupción, pérdida y/o emergencia de las operaciones.

En seguridad de la información es uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones o amenazan la seguridad de la información.

4.21 Integridad
Propiedad de la información que consiste en salvaguardar o mantener la exactitud de los activos de información.

4.22 Oportunidad
Es un evento con impacto positivo en el cumplimiento de los objetivos institucionales.

4.23 Plan de Gestión del Riesgo
Documento que permite definir el curso de acción (lineamientos, actividades y procedimientos), organizar, prever y estimar los recursos (humanos, presupuestarios, materiales y tecnológicos, entre otros), que se requieren para su ejecución; considera las actividades del Proceso Gestión del Riesgo, incluyendo el Plan de Contingencia para los riesgos críticos como parte del Tratamiento del Riesgo.

4.24 Plan de Contingencia
Contiene las acciones de ejecución inmediata en respuesta al riesgo materializado. Es formulado por el Gestor del Riesgo.

4.25 Plan Nacional de Integridad y Lucha contra la Corrupción 2018 - 2021
Norma legal aprobada con Decreto Supremo Nº 044-2018-PCM, que permite la articulación y coordinación entre entidades para la implementación de la Política Nacional de Integridad y Lucha contra la Corrupción. Establece las metas, indicadores y acciones que deberán realizarse para cumplir con los objetivos, en cada uno de los tres Ejes definidos en la Política de Integridad y Lucha contra la Corrupción. Como estrategia de implementación para efectos de facilitar a las entidades públicas la implementación de una estructura de prevención de la corrupción, se plantea un modelo de integridad cuyo desarrollo corresponde a estándares internacionales y buenas prácticas con la finalidad de mejorar la organización de la administración pública para promover la integridad y luchar contra la corrupción. Dispone, que las máximas autoridades de las entidades públicas responsables en el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021 deben adoptar, en el ámbito de sus competencias, las medidas necesarias para su ejecución y velarán por su cumplimiento, asegurando que las acciones y los gastos se incluyan en sus Planes Operativos y Presupuestos Institucionales.

4.26 Política de la Gestión del Riesgo
Declaración de lineamientos o intenciones para la toma de decisiones de la Entidad con respecto a la Gestión del Riesgo; debe ser expresada formalmente por la Alta Dirección.

4.27 Política Nacional de Integridad y Lucha contra la Corrupción
Norma legal aprobada con Decreto Supremo Nº 092-2017-PCM, es de cumplimiento obligatorio para todas las entidades de los diferentes Poderes del Estado, Organismos Constitucionales Autónomos y de los diferentes niveles de gobierno, quienes deben adecuar su marco normativo a la presente norma. También es de obligatorio cumplimiento para el sector privado y la sociedad civil,

en cuanto le sea aplicable y, en lo que no, le sirve como un instrumento guía u orientador. Establece los objetivos, metas, responsables y lineamientos para lograr la prevención y lucha contra la corrupción de manera intersectorial e intergubernamental; establece como objetivo general la necesidad de contar con instituciones transparentes e íntegras que practican y promueven la probidad en el ámbito público, sector empresarial y la sociedad civil; y garantizar la prevención y sanción efectiva de la corrupción a nivel nacional, regional y local, con la participación activa de la ciudadanía. Se organiza en tres ejes: Eje 1 Capacidad preventiva del Estado frente a los actos de corrupción. Eje 2 Identificación y Gestión de Riesgos. EJE 3: Capacidad sancionadora del Estado frente a los actos de corrupción.

4.28 Probabilidad
Posibilidad de que algo suceda, se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos.

4.29 Proceso Gestión Integral del Riesgo
Comprende la realización de actividades necesarias para la mitigación 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.

4.30 Riesgo
Es la posibilidad de ocurrencia de un evento adverso o positivo, que afecte o genere una oportunidad, respecto al cumplimiento de los objetivos institucionales (en los niveles: operacional, táctico y estratégico).
Efecto de la incertidumbre sobre la consecución de los objetivos.

4.31 Riesgo Aceptado
Es el riesgo que la Entidad acepta de acuerdo con su política de Gestión Integral del Riesgo.

4.32 Riesgo Residual
Es el riesgo remanente después de implementar el tratamiento del riesgo.

4.33 Seguimiento, Medición y Control
Proceso de seguimiento permanente y evaluación periódica de la gestión del riesgo en la entidad a cargo de la OFCR y OSDN (a través de la Sub Gerencia de Seguridad de la Información) de acuerdo a su competencia.

4.34 Seguimiento y Revisión
Proceso de seguimiento permanente y evaluación periódica de la gestión del riesgo en la entidad a cargo de los Gestores del Riesgo.

4.35 Servicio Digital
Es aquel provisto de forma total o parcial a través de internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

4.36 Tolerancia al Riesgo

Son los límites superior e inferior aceptables de desviaciones relativas a la consecución de metas y objetivos. Operar dentro de las tolerancias del riesgo proporciona una mayor confianza de que la Entidad permanece dentro de su riesgo aceptado; a la vez, proporciona una mayor seguridad de que la Entidad alcanzará sus objetivos.

4.37 Vulnerabilidad

Ausencia o debilidad de un control que puede ser explotado por una o más amenazas.

V. METODOLOGÍA Y APLICACIÓN DE LA GESTIÓN INTEGRAL DEL RIESGO

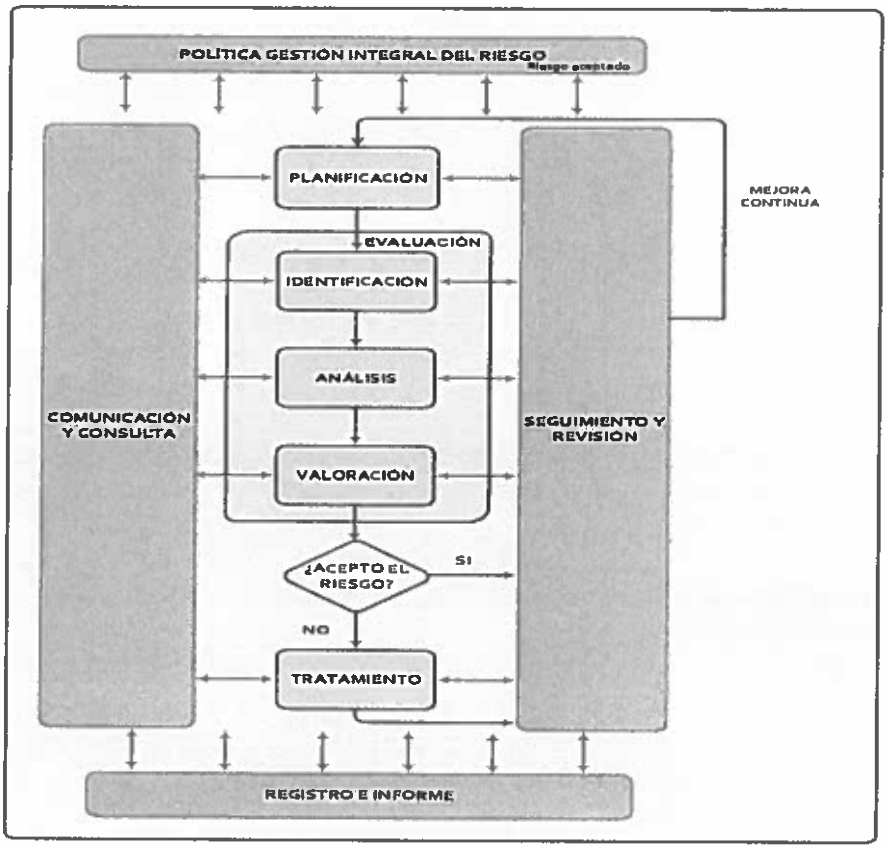
Las organizaciones se han transformado profundamente en los últimos años. Por un lado, el desarrollo de los mercados empujados por los llamados procesos de liberalización e innovación (sobre todo innovación tecnológica) y, por otro, los avances específicos en las regulaciones, conocimiento y gestión de los riesgos, han facilitado la adopción de nuevos y más eficaces enfoques de gestión.

Por lo mencionado, la Gestión del Riesgo se aplica en amplios sectores de la producción industrial y los servicios, de acuerdo a lineamientos establecidos en sistemas de gestión y control, como las ISO y el COSO, y la eficacia de su implementación se logra con la aplicación del proceso de Gestión Integral del Riesgo para lograr la mitigación de todos los tipos de riesgos que se podrían identificar en la entidad.

El RENIEC cuenta con un Sistema de Gestión de Seguridad de la Información y requiere gestionar los riesgos de seguridad de la información siendo el Órgano competente, OSDN (a través de la Sub Gerencia de Seguridad de la Información), quien formulará los documentos normativos y formatos complementarios para su gestión.

El Proceso de Gestión Integral del Riesgo se describe en el siguiente gráfico:

Gráfico N° 01: Proceso Gestión Integral del Riesgo



Fuente: Elaboración OFCR, con referencia NTP-ISO 31000:2018.

El Proceso de Gestión Integral del Riesgo comprende las siguientes actividades:

5.1 PLANIFICACIÓN

La planificación consiste en decidir cómo abordar y llevar a cabo 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 ALCANCE

El propósito del alcance es adaptar el proceso de la Gestión del Riesgo, para permitir una apropiada evaluación y un tratamiento eficaz del riesgo.

La entidad debe definir el alcance de sus actividades de Gestión Integral del Riesgo, considerando su aplicación en los niveles estratégico, táctico y operacional; principalmente, en sus procesos, proyectos, los Sistemas de Gestión con certificaciones ISO u otras actividades como la toma de decisiones, la seguridad de la infraestructura y personas, la continuidad operativa; en alineamiento a los objetivos de la organización.

Este alcance es coherente con el desarrollo y ejecución de la política de riesgos alineada con sus objetivos estratégicos. Su implantación (en los niveles estratégico, táctico y operativo) se realiza como componente del Sistema de control interno y un enfoque de integración en los procesos; a fin de garantizar el cumplimiento de los objetivos propuestos con eficacia y atendiendo las necesidades de las partes interesadas, con énfasis en la atención de los ciudadanos.

El desarrollo de un adecuado ambiente interno, para la Gestión Integral del Riesgo, es promovido por la Alta Dirección, el Comité de Control Interno, y Gerencias de la entidad, como esencial para la asignación de responsabilidades de las actividades referidas al riesgo y la generación del pensamiento basado en riesgos como parte de la cultura de la entidad.

La declaración del compromiso por parte de los funcionarios y servidores públicos, ayuda a que la gestión de riesgos se integre en todos los niveles de la entidad.

5.1.2 MARCO DE REFERENCIA

Para que la gestión del riesgo se incorpore en todas las actividades y funciones significativas, se debe implementar el marco de referencia de la Gestión Integral del Riesgo. La eficacia de la Gestión integral del riesgo dependerá de su integración en la gobernanza de la organización incluyendo la toma de decisiones, por tanto, se requiere del liderazgo y compromiso permanente de la Alta Dirección, los órganos de supervisión y el apoyo de las partes interesadas.

El desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la Gestión Integral del Riesgo a lo largo de toda la entidad.

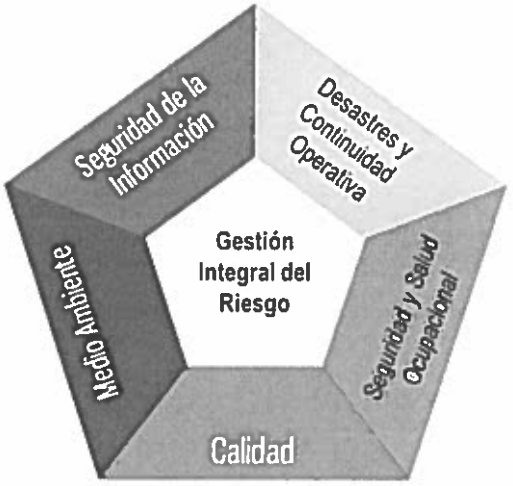
Gráfico N° 02: Marco de Referencia de la GIR

Fuente: NTP-ISO 31000:2018.

✓ **Integración:**

El modelo de la Gestión Integral del Riesgo es el eje articulador que facilita la gestión integrada de otros sistemas de gestión tales como: gestión de la calidad, gestión ambiental, gestión de la seguridad y salud ocupacional, seguridad de la información, desastres y continuidad operativa, o cualquier otro sistema de gestión basado en el ciclo PDCA y la mejora continua.

Gráfico N° 03: Articulación de los sistemas de gestión



Fuente: Elaboración OFCR

La integración de sistemas de gestión no necesariamente significa una mera incorporación o fusión de sistemas de gestión, sino que puede resultar algo más complejo, donde el gran sistema de la entidad dispone de varios sistemas, cada uno posee un objetivo que permanece alineado para cubrir las expectativas de la alta dirección y de las partes interesadas, confluyen de diferentes ámbitos y se incorporan a un solo entorno, conservando las particularidades de las normas o regulaciones que los rigen. La unificación de objetivos y propósitos contribuye a un enfoque de trabajo en equipo enlazando el concepto sinérgico de la utilización de recursos.

✓ **Diseño:**

- **Comprensión de la entidad y su contexto**: Se deberá analizar y comprender los contextos interno y externo cuando se diseñe el marco de referencia para gestionar el riesgo, teniendo en cuenta las situaciones del entorno de la entidad y todas sus partes interesadas. La adecuada elaboración del contexto facilita la identificación, análisis y evaluación de los riesgos.

  El contexto interno

  Considera:

  ✓ La gobernanza.

- ✓ Fijar la Política y los objetivos estratégicos y operativos de la Gestión integral del riesgo con un enfoque de integración de los procesos, desplegándola a todo nivel.
- ✓ El modelo de gestión de Riesgos incorporado a la Planificación estratégica (misión, visión, valores, liderazgo, estructura organizacional y cultura organizacional).
- ✓ Definir los Procesos, planes, proyectos, activos, sistemas de gestión, procesos para la toma de decisiones
- ✓ Asignar roles, autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados de la organización, permitirá alinear la gestión del riesgo con sus objetivos, estrategias y cultura organizacional.
- ✓ Administrar los recursos (Capacidades y competencias del personal, condiciones de trabajo, sistemas de información y tecnologías, flujos de información), la Alta Dirección y los órganos de supervisión deberán asegurar la asignación los recursos apropiados para la gestión del riesgo.
- ✓ Establecer mecanismos de comunicación interna y externas de acuerdo al contexto de la organización, normativas y relaciones contractuales, que permitan percibir las necesidades y expectativas de las partes interesadas.
- ✓ Las principales fuentes de consulta a utilizar son: PEI, POI, ROF, MOF, CAP, PAP, PDP, Mapa de Procesos, Planes de Trabajo de Control Interno; otros informes, planes, programas, proyectos de importancia institucional que permitan conocer o determinar los objetivos y resultados sobre los que impacta el riesgo.

El contexto externo (Nacional, regional, local e internacional) atribuye aspectos: culturales, sociales, políticos, legales, reglamentarios, financiero, tecnológico, económico, medioambientales, etc. Tendencias e impulsores con impacto en objetivos institucionales. Percepciones, valores, necesidades y expectativas de partes interesadas externas. Comunicación e información externa.

El análisis del contexto externo e interno, las partes interesadas, deben ser registradas en el **Registro Análisis del Contexto y Partes Interesadas - Anexo N° 01**.

- **Articulación del Compromiso de la Gestión Integral del Riesgo**: La Alta Dirección y los órganos de la entidad deberán articular y demostrar su compromiso, expresándose claramente mediante una política, una declaración u otras formas, incluyendo la integración de la gestión de riesgos a la cultura organizacional y la toma de decisiones.
- **Asignar roles, autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados de la organización:** permitirá alinear la gestión del riesgo con sus objetivos, estrategias y cultura organizacional.

- **Establecimiento de la comunicación y consulta:** La comunicación implica compartir información con las partes interesadas, asimismo es importante efectuar consultas respecto a las necesidades y expectativas de las partes interesadas. La entidad definirá los mecanismos de comunicación y consulta pertinentes, para cuyo efecto los gestores del riesgo deberán identificar las partes interesadas (ciudadanos, empresas, instituciones, entre otros), vinculados a sus procesos y actividades, recogiendo sus necesidades y expectativas.

✓ **Implementación:** La entidad debería implementar el marco de referencia de la gestión del riesgo mediante el desarrollo de un plan apropiado incluyendo plazos y recursos; la identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización; la modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario; el aseguramiento de que las disposiciones de la entidad para gestionar el riesgo son claramente comprendidas y puestas en práctica.

✓ **Valoración:** Para valorar la eficacia del marco de referencia de la gestión del riesgo, la entidad deberá medir periódicamente su desempeño con relación a su propósito, planes para la implementación, indicadores y el comportamiento esperado, determinando su idoneidad para apoyar el logro de los objetivos de la organización.

✓ **Mejora:** Realizar el seguimiento continuo y adaptar el marco de referencia de la gestión del riesgo en función de los cambios externos e internos, de esta manera debe mejorarse su valor.

5.1.3 CRITERIOS DEL RIESGO

La entidad de acuerdo a su naturaleza organizacional, determina la cantidad y tipo de riesgos, habiéndose considerando aquellos que se encuentran relacionados a sus procesos y actividades: riesgos de corrupción, cumplimiento, desastres, estratégico, financiero, imagen, medio ambiente, operativo, proyectos, seguridad de la información, seguridad y salud en el trabajo, tecnológico y otros que correspondan a la entidad.

Asimismo, se establece el apetito por el riesgo en la política aprobada de acuerdo a sus objetivos, valores, requisitos legales o normativos u otros suscritos por la entidad que deben tenerse en cuenta para valorar la importancia del riesgo y para apoyar la toma de decisiones.

Además, se definieron la probabilidad e impacto, el nivel del riesgo, los mismos que se detallan en el procedimiento de cada etapa del proceso de la Gestión Integral del Riesgo del presente manual.

En el caso de los riesgos de Seguridad y Salud en el Trabajo, serán gestionados de acuerdo a las normas internas específicas y vigentes.

En acotación a los riesgos de corrupción, es importante mencionar que el Decreto Supremo N° 044-2018-PCM, que aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021 en el EJE 2. Identificación y Gestión de Riesgos, considera como una de sus acciones,

desarrollar una metodología específica de identificación y gestión del riesgo de corrupción, que incluya actividades de mapeo y evaluación adaptadas para apoyar a las entidades gubernamentales en sus esfuerzos por implementar controles para prevenir, detectar y responder eficazmente a la corrupción, dicha metodología será incorporada al presente manual en cuanto la PCM-CAN lo apruebe.

5.1.4 IDENTIFICACIÓN DEL PROCESO

La identificación y priorización del proceso tiene como objetivo establecer el nivel de contribución que realiza un determinado proceso al cumplimiento de los objetivos institucionales el cual **debe** ser registrado en el **Registro para Priorización de Procesos - Anexo N° 01**, para lo cual debe utilizar el Cuadro N° 01: Nivel de contribución del proceso.

Cuadro N° 01: Nivel de Contribución del Proceso

CLASIFICACION DEL NIVEL	NIVEL DE CONTRIBUCION DEL PROCESO	VALOR DE ALINEACIÓN CON LOS OEI	RANGO PARA DETERMINAR EL NIVEL DE CONTRIBUCIÓN DEL PROCESO
ALTO	El proceso aporta de manera **fundamental** en el cumplimiento del objetivo estratégico	3	2.01 - 3
MEDIO	El proceso aporta de manera **importante** fundamental en el cumplimiento del objetivo estratégico	2	1.01 - 2
BAJO	El proceso aporta de manera **mínima** en el cumplimiento del objetivo estratégico	1	0.1 - 1
NULO	El proceso no aporta en el cumplimiento del objetivo estratégico	0	0

A continuación, se muestra el ejemplo de llenado del Registro:

PROCESO INSTITUCIONAL	ÓRGANO	PROCESOS DEL ÓRGANO	ALINEAMIENTO A LOS OBJETIVOS ESTRATÉGICOS INSTITUCIONALES					RESULTADO DEL NIVEL DE CONTRIBUCION DEL PROCESO AL CUMPLIMIENTO DE LOS OEI (PROMEDIO)
			OEI 1 Fortalecer los servicios de registros de la identidad y de la identificación en beneficio de la población	OEI 2 Mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad	OEI 3 Intensificar los procesos para la identidad y la identificación digital de la población	OEI 4 Fortalecer la gestión institucional	OEI 5 Fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución	
REGISTRO DE LA IDENTIFICACION	GOR	CAPTURA	3	2	3	1	2	2.2
		ENTREGA	3	2	3	1	2	2.2
		DESPACHO	1	1	2	1	1	1.2
	GRI	DIGITALIZACIÓN	3	2	3	1	1	2
		EVALUACION	2	2	2	1	1	1.6
		IMPRESIÓN	3	2	3	1	1	2

En este formato se identifica el proceso, el órgano u órganos responsables de su

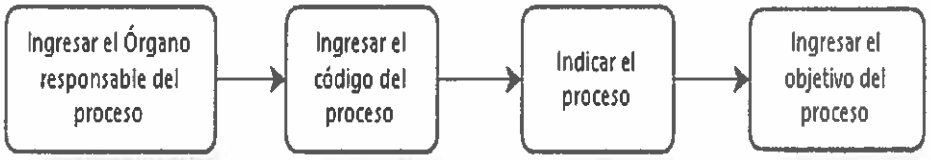
ejecución, y se valora de 0 a 3, donde a mayor valor del número significa un mayor nivel de aporte al objetivo institucional correspondiente. Como resultado se obtiene un promedio simple que determina el nivel de criticidad del proceso a cargo del órgano. Así, aquellos que obtengan un nivel medio o alto, tendrán prioridad para la gestión de sus riesgos.

Es importante precisar que la priorización no excluye a los procesos restantes para la Gestión Integral del Riesgo, siendo necesario se identifiquen los riesgos en todos los procesos.

El **Plan de Gestión Integral del Riesgo - Anexo N° 01**, contiene todas las etapas del proceso de Gestión Integral del Riesgo.

En la etapa identificación de proceso se **debe** registrar información correspondiente al proceso como: órgano responsable del proceso, el código del proceso (definido en la ingeniería de procesos de la entidad), el nombre del proceso y su objetivo. A continuación, se muestra un flujo de la información a registrar.

Gráfico N° 04: Identificación del Proceso



Fuente: Elaboración OFCR.

A lo largo del presente manual se mostrará un ejemplo de aplicación relacionado al proceso de "Entrega de DNI" a cargo de la Gerencia de Operaciones Registrales.

Ejemplo:

ÓRGANO RESPONSABLE DEL PROCESO	CÓDIGO DEL PROCESO	PROCESO	OBJETIVO DEL PROCESO
GOR	(*)	Entrega de DNI en locales RENIEC	Entregar el DNI a los ciudadanos cumpliendo los procedimientos establecidos.

(*) Los códigos de los procesos serán asignados de acuerdo a la Ingeniería de procesos de la entidad.

5.2 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 lograr sus objetivos, para ello es importante contar con información apropiada y actualizada.

Para identificar el riesgo en el proceso se **debe** considerar el contexto externo e interno para lo cual se **debe** utilizar el Registro **de Análisis de Contexto y Partes Interesadas - Anexo N° 01,** teniendo presente los objetivos para precisar el alcance del proceso, proyecto, producto, servicio, activo, sistema de gestión u otros.

De igual forma, se **debe** analizar y registrar en el **Anexo N° 01,** el efecto o consecuencias en el proceso, actividades y tareas, considerando su locación; teniendo en cuenta el comportamiento y capacidades humanas, la organización del trabajo y otros factores humanos; servicios de apoyo y equipamiento en la organización; la gestión de proveedores y la subcontratación de actividades; la infraestructura, productos y/o servicios; los cambios o propuestas de cambio en la entidad.

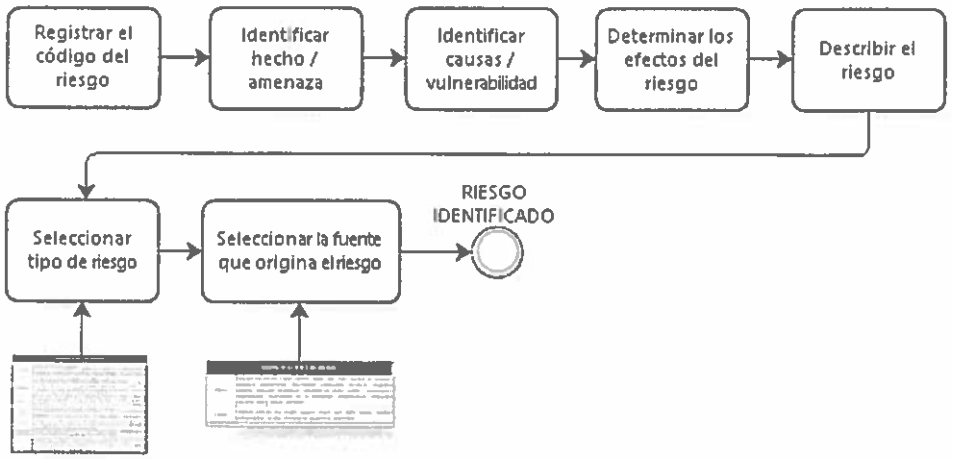
Para la identificación de riesgos se **debe** seleccionar uno de los métodos del **Anexo N° 02 - Técnicas utilizadas en la gestión del riesgo**, que mejor se adapten a los recursos humanos y sus capacidades; a la naturaleza y grado de incertidumbre y a la complejidad de los riesgos.

Las actividades que **debe** realizar el Coordinador del riesgo o Gestor Líder conjuntamente con el Equipo de Riesgos en la etapa de identificación del riesgo en su proceso, serán las siguientes:

Nro. de Actividad	Descripción de la actividad
1	Ingresar el código de riesgo de acuerdo a la siguiente estructura: CODIGO DEL PROCESO + "_" + R + Número Correlativo **EJEMPLO: P08.01.03.03_R01** **DONDE:** **CODIGO DEL PROCESO:** Es el código asignado a cada proceso por el Comité de Procesos de la entidad. "_": Guion bajo que separa el código del proceso de la numeración del riesgo. **R:** Es una constante que indica la identificación de un Riesgo. **Número Correlativo:** inicia en 01, 02, 03...
2	Identificar y describir el **hecho o amenaza (para riesgos de Seguridad de la información y Desastres).**
3	Identificar y registrar las **causas o vulnerabilidades (para riesgos de Seguridad de la información y Desastres)** del riesgo, las circunstancias y agentes generadores, los cuales pueden ser: personas, materiales, tecnología, instalaciones, entorno, entre otros. Las causas pueden ser intencionales o no.
4	Registrar los **efectos** o consecuencias del riesgo materializado.
5	Registrar la **descripción del riesgo** de acuerdo a la siguiente estructura: Debido a la **<CAUSA/VULNERABILIDAD>** puede ocurrir el **<HECHO / AMENAZA/RIESGO>**, lo que provocaría el **<EFECTO o CONSECUENCIA>**

6	Seleccionar el tipo de riesgo de acuerdo a la Tabla N° 1.1 Tipo de Riesgo - Anexo N° 03
7	Para riesgo de Proyecto: Seleccionar la categoría de acuerdo a la Tabla N° 1.2 Categoría de Riesgo de Proyecto - Anexo N° 03
8	Seleccionar la fuente del riesgo según su origen (interno o externo). Tabla N° 02 Fuente del Riesgo - Anexo N° 03

Gráfico N° 05: Identificación del Riesgo



Fuente: Elaboración OFCR.

Ejemplo: Continuando con el caso anterior, se muestra un modelo de registro de los campos mencionados:

IDENTIFICACIÓN DEL RIESGO						
CÓDIGO DEL RIESGO	**HECHO O AMENAZA (para riesgos de Seguridad de la Información, Desastres y SST)**	**CAUSAS O VULNERABILIDAD**	**EFECTOS**	**DESCRIPCIÓN DEL RIESGO**	**TIPO DE RIESGO (TABLA 1)**	**FUENTE QUE ORIGINA EL RIESGO (TABLA 2)**
P08.01.03.03_ R01		♦ Desconocimiento del procedimiento en la entrega de DNI por falta de capacitación. ♦ Incumplimiento del procedimiento. ♦ GP-269-GOR/004 "Registros de Trámite y entrega del Documento Nacional de Identidad" desactualizada. ♦ Error del registrador en el proceso de entrega del DNI. ♦ Colusión del registrador con tercera persona. ♦ No contar con lectores biométricos en todos los locales RENIEC.	♦ Afectación al ciudadano. ♦ Demanda al RENIEC por parte del ciudadano. ♦ Perjuicio económico a RENIEC por el pago de indemnización al ciudadano. ♦ Afectación a la imagen institucional.	Deficiencias en la verificación de la identidad durante la entrega del DNI de mayor de edad en los locales de atención, podría ocasionar que el documento nacional de identidad sea entregado a persona distinta del titular generando perjuicio al ciudadano por uso indebido.	OPERATIVO	INTERNA

5.3 ANÁLISIS Y VALORACIÓN DEL RIESGO

5.3.1 ANÁLISIS DEL RIESGO

Consiste en determinar la probabilidad y el impacto o consecuencias.

El Análisis del riesgo **debe** considerar factores tales como:

- La probabilidad de los eventos o posibilidad de ocurrencia, en términos de frecuencia (eventos ocurridos en un determinado periodo de tiempo) o factibilidad (presencia de factores externos – internos que pueden propiciar el riesgo), para la evaluación de la probabilidad se **debe** utilizar la **Tabla N°3** de **Probabilidad - Anexo N° 03.**

- El impacto o consecuencias que afectan a los objetivos pueden ser negativas o positivas; para la evaluación del impacto se **debe** utilizar la **Tabla N°4.1 Impacto para riesgos en General, Tabla N°4.2 Impactos para riesgos en Seguridad de la Información** y la **Tabla N°4.3 Impacto para riesgo de Proyectos - Anexo N° 03**, según corresponda al tipo de riesgo. En el presente manual se han definido los siguientes criterios de impacto:

  - ✓ **Resultados y Objetivos Institucionales**; el grado en que el riesgo afecta los resultados y el cumplimiento de los objetivos institucionales. Como referencia se tendrá en cuenta el cumplimiento del PEI y POI.
  - ✓ **Cumplimiento Legal y Normativo**; cómo afecta el riesgo al cumplimiento legal (externo) y normativo (interno), acuerdos con las partes interesadas, existiendo posibilidad de multas, sanciones, demandas, observaciones-recomendaciones, penalidades contractuales u otros similares.
  - ✓ **Imagen Institucional**; cómo afecta el riesgo la percepción y confianza de los ciudadanos sobre la reputación de la entidad. También considera la percepción de otras partes interesadas.
  - ✓ **Operatividad**; el grado de afectación a las actividades de los procesos, si el riesgo puede ocasionar la interrupción de los servicios que brinda la entidad.
  - ✓ **Recursos disponibles y costos**; cómo es que afecta los recursos asignados y el costo del daño y la recuperación según la magnitud de los daños.
  - ✓ **Medioambiente**; cuando ocasiona daños al medioambiente.
  - ✓ **Sistemas de Gestión de la calidad y otros**; como afecta el sistema de gestión de calidad con posible pérdida de la certificación.
  - ✓ **Seguridad de la Información y Seguridad Digital**; el grado en que ocasiona la pérdida parcial o total de la Confidencialidad, Integridad y/o Disponibilidad (CID), afectando el entorno digital o físico con pérdida de la información.
  - ✓ **Competencias para la Gestión del Riesgo**; el grado en que el personal cuenta con las competencias necesarias para contribuir con la gestión del riesgo.

La probabilidad y el impacto o consecuencias se combinan para determinar un **nivel de riesgo inherente o sin control;** el cual puede ser admisible, tolerable, moderado, importante o crítico. **Tabla N° 05 Matriz de Probabilidad e Impacto o mapa de Calor - Anexo N°03.**

En esta etapa se **debe** realizar la evaluación del control y/o controles existentes en el **Registro de Evaluación de Controles existentes/implementados – Anexo N° 01**, para lo cual se **debe** utilizar las **Tabla N° 06 Tipos de Control existente/implementado, Tabla N° 07 Criterios para el análisis del control existente/implementado** y la **Tabla N° 08 Rangos del resultado de la calificación del control existente/implementado - Anexo N° 03.**

El tipo de control seleccionado y el resultado de la calificación del control existente permiten obtener el **nivel de exposición del riesgo con control.**

5.3.2 VALORACIÓN DEL RIESGO

La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios (Política y objetivos de la Gestión Integral del Riesgo); para tomar una decisión, la cual puede conducir a:

- ✓ No hacer nada más;
- ✓ Considerar opciones para el tratamiento del riesgo;
- ✓ Realizar un análisis adicional para comprender mejor el riesgo;
- ✓ Mantener los controles existentes;
- ✓ Reconsiderar los objetivos.

Esta comparación determina la decisión sobre la necesidad, prioridad, recursos y características del Tratamiento.

Las actividades que **debe** realizar el Coordinador del riesgo o Gestor Líder y el Equipo de Riesgos en la etapa de análisis y valoración del riesgo en su proceso, serán las siguientes:

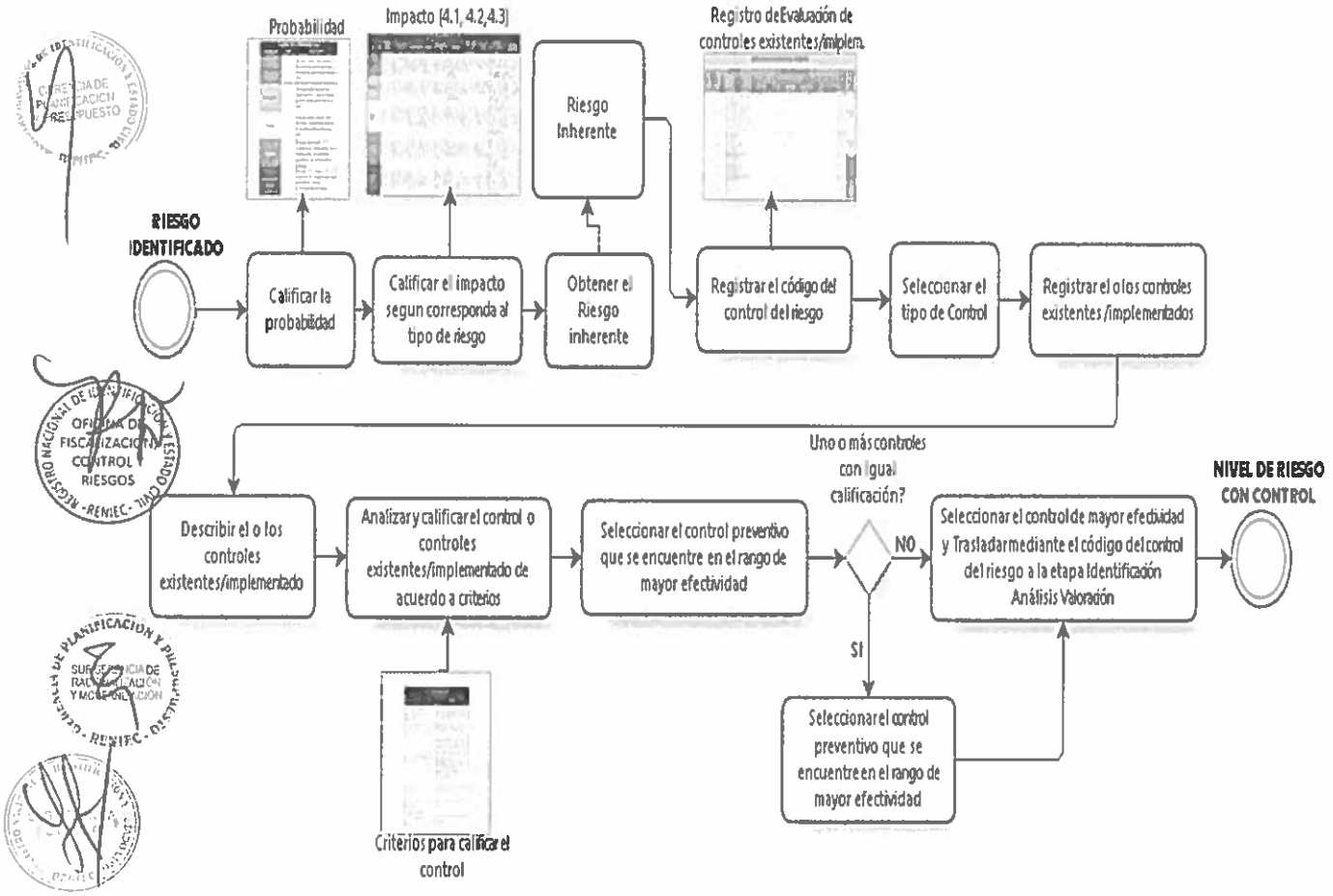
Nº de Actividad	Descripción de la actividad
9	Seleccionar y calificar la probabilidad de ocurrencia utilizando la **Tabla N° 03 de Probabilidad - Anexo N° 03.**
10	Calificar el impacto de acuerdo a los criterios establecidos en las Tablas **N° 4.1, 4.2 y 4.3 - Anexo N° 03**, según corresponda por el tipo de riesgo. Como resultado de la calificación de la probabilidad por el impacto obtenemos el Nivel del riesgo inherente el cual se podrá visualizar en la **Tabla N° 05 Matriz de Probabilidad e Impacto o Mapa de Calor - Anexo N° 03.**
11	Registrar el o los controles existentes según corresponda, para lo cual debe utilizar el **Registro Evaluación de Controles existente/implementados – Anexo N° 01.**
12	En el Registro Evaluación de Controles del **Anexo N° 01** se **debe** realizar lo siguiente: 11.1 Registrar el código del control del riesgo. 11.2 Seleccionar el tipo de control, para lo cual debe utilizar la **Tabla N° 06 Tipos de Control Existente/implementado - Anexo N° 03.** 11.3 Registrar el código del control. 11.4 Describir el control o controles existentes, el mismo que deberá responder a las preguntas: **¿Qué** control se realiza**?;** **¿Cuál** es el documento que describe el control**?;** **¿Cómo** se realiza el control**?;** **¿Quién** realiza el control**?;**

	¿Cuándo se realiza el control? 11.5 Calificar el control o controles existentes de acuerdo a la **Tabla N° 07: Criterios para el Análisis del Control Existente/implementado - Anexo N° 03.** 11.6 Seleccionar el control con mayor nivel de efectividad de acuerdo a la **Tabla N° 08 Rangos del resultado de la calificación del control existente / implementado – Anexo N° 03 (*).** 11.7 Trasladar los datos del control seleccionado al **Registro de Identificación Análisis Valoración – Anexo 01**, Registrando el código del control del riesgo.

(*) De obtener uno (1) o más controles con igual calificación (efectividad de control) deberán seleccionar el control preventivo que se encuentre en el rango de mayor efectividad.

Como resultado de estas actividades se **debe** obtener el **nivel de exposición del riesgo con control** que nos servirá para tomar una decisión para el tratamiento del riesgo.

Gráfico N° 06: Análisis y Valoración del riesgo



Fuente: Elaboración OFCR.

Continuando con el Ejemplo del proceso "Entrega de DNI en los locales RENIEC". Seleccionar y calificar el nivel de probabilidad.

CALCULO DE LA PROBABILIDAD	
PROBABILIDAD (TABLA 3)	VALOR
POSIBLE	3

MUY IMPROBABLE
IMPROBABLE
POSIBLE
PROBABLE
PRÁCTICAMENTE SE

Seleccionar y calificar el impacto de acuerdo a los criterios establecidos, según corresponda por el tipo de riesgo.

CRITERIOS DE IMPACTO (TABLA N° 4.1)							
RESULTADOS Y OBJETIVOS INSTITUCIONALES	CUMPLIMIENTO LEGAL Y NORMATIVO	IMAGEN INSTITUCIONAL	OPERATIVIDAD	RECURSOS DISPONIBLES Y COSTOS	MEDIOAMBIENTE	SISTEMAS DE GESTION	COMPETENCIAS EN LA GESTION DEL RIESGO
MODERADO O MEDIO	MODERADO O MEDIO	GRAVE O ALTO	LEVE O BAJO	LEVE O BAJO	INSIGNIFICANTE O MUY BAJO	MODERADO O MEDIO	LEVE O BAJO

INSIGNIFICANTE O MUY BA
LEVE O BAJO
MODERADO O MEDIO
GRAVE O ALTO
CATASTROFICO O MUY AL

Como resultado de la calificación de la probabilidad por el impacto obtenemos el Nivel del riesgo inherente

RESULTADO DEL IMPACTO	VALOR	P X I	RIESGO INHERENTE
GRAVE O ALTO	4	12	IMPORTANTE

En la **"matriz de probabilidad e impacto" o "mapa de calor"** se puede visualizar la intersección de la probabilidad e impacto para este Ejemplo.

MATRIZ DE PROBABILIDAD E IMPACTO O MAPA DE CALOR
(PROBABILIDAD x IMPACTO)

PROBABILIDAD							
	Practicamente Seguro	5	TOLERABLE	MODERADO	IMPORTANTE	CRÍTICO	CRÍTICO
	Probable	4	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE	CRÍTICO
	Posible	3	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE
	Improbable	2	ADMISIBLE	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE
	Muy Improbable	1	ADMISIBLE	ADMISIBLE	TOLERABLE	MODERADO	MODERADO
			1	2	3	4	5
			Insignificante o Muy Bajo	Leve o Bajo	Moderado o Medio	Grave o Alto	Catastrófico o Muy alto
			IMPACTO				

En el Registro Evaluación de Controles se **debe r**egistrar el código del control del riesgo, seleccionar el tipo de control y describir el control o controles existentes

CODIGO DEL CONTROL DEL RIESGO	CONTROL EXISTENTE	
	TIPO DE CONTROL EXISTENTE (TABLA 6)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA 7)
P08.01.03 03_C001	CORRECTIVO	Qué: Homologación y/o validación de imágenes (firma e impresión dactilar Cuál: GP-269-GOR/004 Registros de Trámite y Entrega del Documento Nacional de Identidad Quién: El registrador de entregas de DNI. Cómo: Verificación de las imágenes capturadas versus la información del sistema Cuándo: Permanente en cada entrega de DNI

Calificar el control o controles existentes de acuerdo a los criterios establecidos, como resultados se obtiene la calificación y efectividad del control

CRITERIOS PARA EL ANALISIS DEL CONTROL EXISTENTE												CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA 8)
¿Existe un medio documentado vigente y actualizado para la aplicación del control?		¿Se han definido (s) de la responsable ejecución del control?		¿Cuál es el tipo de aplicación de control que se realiza?		¿Se ha definido la frecuencia de aplicación del control?		¿Se cuenta con evidencias de la ejecución y seguimiento del control?		¿En el tiempo que lleva la aplicación del control ha demostrado ser efectiva?			
SI	20	SI	10	SEMIAUTOMATICO	10	SI	10	SI	25	NO	0	75	PARCIALMENTE EFECTIVO

Trasladar los datos del control seleccionado al **Registro de Identificación Análisis Valoración (Anexo N°1),** registrando el código del control del riesgo de acuerdo al siguiente cuadro.

CONTROL EXISTENTE			CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL ACTUAL (TABLA 8)
CODIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL EXISTENTE (TABLA 6)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA 7)		
P08 01 03 03_C001	CORRECTIVO	Qué: Homologación y/o validación de imágenes (firma e impresión dactilar) Cuál: GP-269-GOR/004 "Registros de Trámite y Entrega del Documento Nacional de Identidad". Quién: El registrador de entregas de DNI. Cómo: Verificación de las imágenes capturadas versus la información del sistema. Cuándo: Permanente en cada entrega de DNI.	75	PARCIALMENTE EFECTIVO

Como resultado obtenemos el nivel de exposición del riesgo con control que nos servirá para tomar una decisión para el tratamiento del riesgo en el caso del ejemplo **el riesgo debe ser tratado.**

NIVEL DE RIESGO CON CONTROL						
PROBABILIDAD (TABLA 3)	VALOR	IMPACTO (TABLA 4)	VALOR	P X I	NIVEL DE RIESGO (TABLA 5)	ACCION A REALIZAR
POSIBLE	3	MODERADO O MEDIO	3	9	MODERADO	EL RIESGO DEBE SER TRATADO

Para el Ejemplo podemos visualizar que se ha reducido la probabilidad en un (1) nivel, de **importante** a **moderado**.

MATRIZ DE PROBABILIDAD E IMPACTO O MAPA DE CALOR (PROBABILIDAD x IMPACTO)							
PROBABILIDAD	Practicamente Seguro	5	TOLERABLE	MODERADO	IMPORTANTE	CRÍTICO	CRÍTICO
	Probable	4	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE	CRÍTICO
	Posible	3	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE
	Improbable	2	ADMISIBLE	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE
	Muy Improbable	1	ADMISIBLE	ADMISIBLE	TOLERABLE	MODERADO	MODERADO
			1	2	3	4	5
			Insignificante o Muy Bajo	Leve o Bajo	Moderado o Medio	Grave o Alto	Catastrófico o Muy alto
			IMPACTO				

5.4 TRATAMIENTO DEL RIESGO

El tratamiento al riesgo tiene como objetivo diseñar, evaluar, seleccionar e implementar acciones para gestionar los riesgos identificados que serán evaluadas en la etapa de seguimiento y revisión.

Una vez identificado el nivel de exposición del riesgo con control, se **debe** utilizar la **Tabla N° 09 Respuesta al riesgo - Anexo N° 03**, para determinar la respuesta al riesgo: **Evitar, Reducir, Compartir o Aceptar.**
Es importante que para determinar la respuesta al riesgo se tome en cuenta la política de Gestión Integral del Riesgo y se prioricen aquellos con un mayor nivel de exposición al riesgo, considerando la evaluación costo – beneficio.

Los riesgos de nivel moderado deben ser implementados prioritariamente con recursos que el área ya cuente: personal, materiales, entre otros, evitando así la adquisición o contratación, que genere nuevos costos para la institución.

En esta etapa se establecen Planes de Tratamiento cuyas acciones tienen el objetivo de reducir el nivel probabilidad y/o impacto del riesgo identificado. En dichos planes se detallan las acciones y controles propuestos, datos personales de los responsables de la aprobación e implementación del plan, los recursos necesarios, los plazos previstos para la realización y la finalización de las acciones.

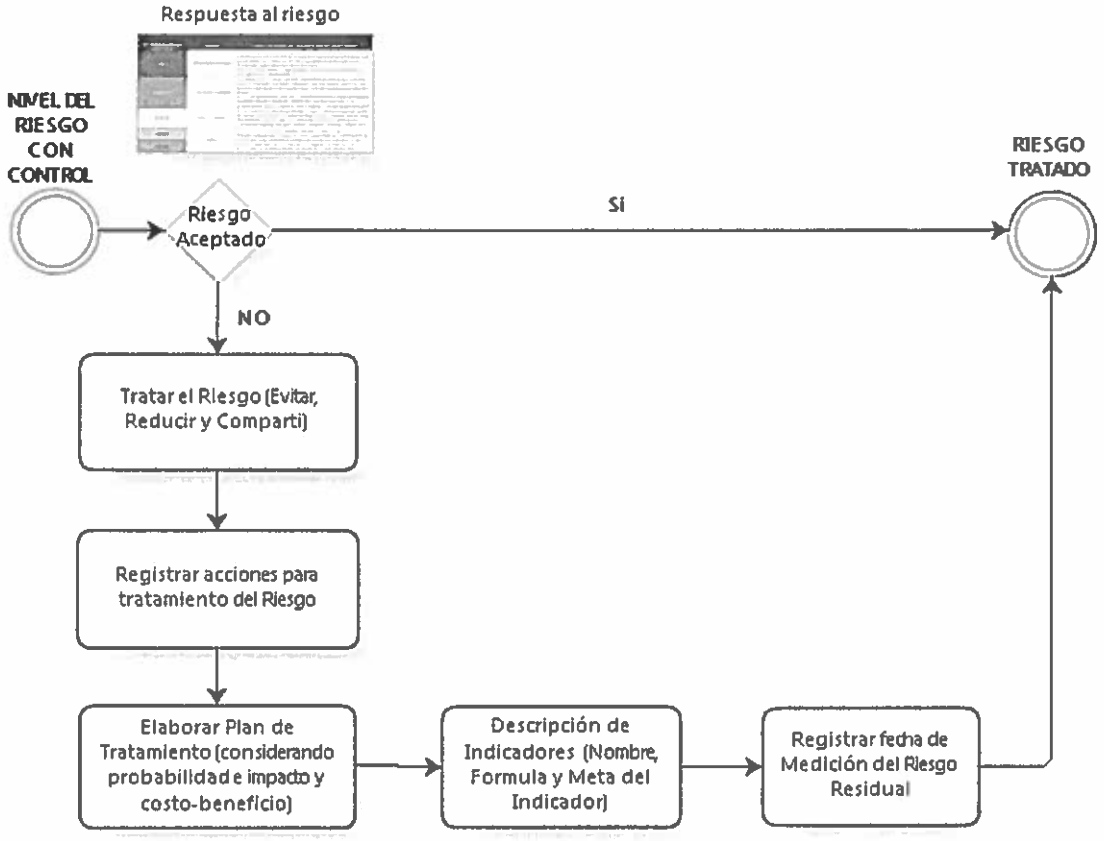
Para los riesgos con niveles de exposición **moderados, importantes y críticos** se **debe** considerar la elaboración o utilización de planes de contingencia en caso se materialice el riesgo.

Las actividades que **debe** realizar el Coordinador del riesgo o Gestor Líder y el Equipo de Riesgos en la etapa de tratamiento del riesgo en su proceso, serán las siguientes:

N° de Actividad	Descripción de la actividad
13	Seleccionar la respuesta para lo cual debe utilizar la **Tabla N° 09 Respuesta al riesgo - Anexo N° 03.**
14	Si la respuesta es Evitar, Reducir o Compartir se deberán establecer acciones de tratamiento, plazos y funcionario responsable de su implementación. **Tabla N° 10 Criterios para la respuesta al riesgo en la etapa de tratamiento - Anexo N° 03.**
15	Describir el indicador relevante del proceso alineado al riesgo identificado, que permita medir el comportamiento del riesgo y la efectividad del control.
16	Registrar la fecha de medición del riesgo residual, el cual debe realizarse a los tres meses después de haber culminado su implementación (para Seguridad de la Información será en coordinación con la efectividad de controles).

Como resultado de estas actividades se **debe** obtener las acciones del tratamiento contenidas en el Plan de Tratamiento del Riesgo.

Gráfico N° 07: Tratamiento del riesgo



Fuente: Elaboración OFCR.

Continuando con el caso del proceso "Entrega de DNI"; en el campo "Respuesta al Riesgo" se **debe** seleccionar una de las respuestas; **evitar, reducir o compartir,** según corresponda.

En el campo correspondiente a las "Acciones Adoptadas para el Tratamiento del Riesgo", se registran las acciones que se propongan para el tratamiento al riesgo, luego de haberse efectuado el análisis y valoración del riesgo identificado, asimismo se **debe** registrar los "Plazos para la implementación de las Acciones", es decir el tiempo estimado a emplearse para implementar cada una de las acciones de tratamiento propuestas (fecha de inicio y fin), considerando que el tiempo estimado sea el adecuado.

Ejemplo:

RESPUESTA AL RIESGO (TABLA 09 Y 10)	ACCIONES ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO	PLAZO PARA LA IMPLEMENTACIÓN DE LAS ACCIONES	
		FECHA DE INICIO	FECHA DE FIN
REDUCIR	1. Adquirir y distribuir los lectores biometricos para la entrega del DNI en los locales de atención. 2. Actualización de la GP-269-GOR/004 "Registros de Trámite y Entrega del Documento Nacional de Identidad". 3. Reforzamiento de los conocimientos del personal respecto a los procedimientos mediante un plan de capacitación.	10/08/2018 10/08/2018 10/03/2019	10/06/2019 10/02/2019 10/06/2019

EVITAR
REDUCIR
COMPARTIR

En los campos siguientes se registran los nombres, apellidos, DNI, cargo y el área del funcionario responsable de adoptar las acciones para el tratamiento del riesgo.

FUNCIONARIO RESPONSABLE DE ADOPTAR ACCIONES PARA EL TRATAMIENTO DEL RIESGO			
NOMBRES Y APELLIDOS	DNI	CARGO	ÁREA RESPONSABLE
CESAR FORTUNATO MENDOZA HERNANDEZ	01020305	GERENTE	GOR

En esta etapa de tratamiento la respuesta **"Aceptar"** solo aparecerá en la lista de respuestas cuando el nivel del riesgo sea **tolerable** o **admisible**, al ser seleccionada dicha respuesta automáticamente se bloquearán los campos de "Acciones Adoptadas para el Tratamiento del Riesgo", "Plazo para la Implementación de las Acciones" (fecha de inicio y fin) y "Funcionario Responsable de Adoptar Acciones para el Tratamiento del riesgo" (nombres y apellidos, DNI, cargo y área responsable).

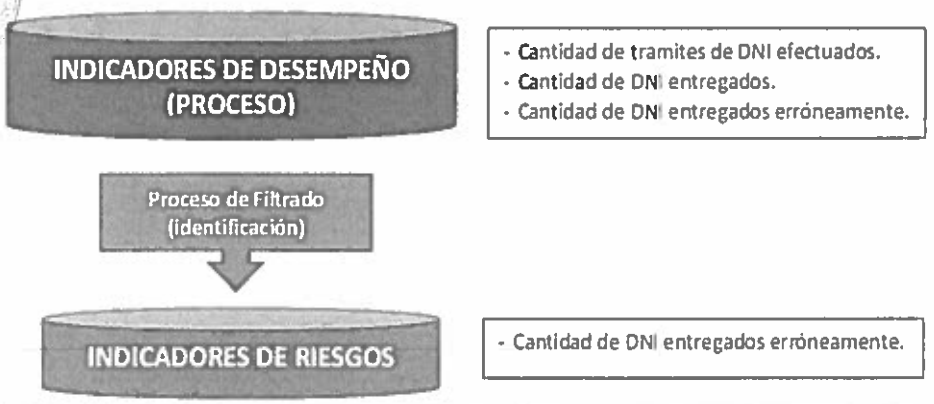
RESPUESTA AL RIESGO (TABLA 10 Y 11)	ACCIONES ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO	PLAZO PARA LA IMPLEMENTACIÓN DE LAS ACCIONES	
		FECHA DE INICIO	FECHA DE FIN
ACEPTAR			

FUNCIONARIO RESPONSABLE DE ADOPTAR ACCIONES PARA EL TRATAMIENTO DEL RIESGO			
NOMBRES Y APELLIDOS	DNI	CARGO	ÁREA RESPONSABLE

Formulación de Indicadores del Riesgo

Para la formulación de los indicadores de Riesgos se **debe** tener como base los indicadores enunciados en los procesos, esto permitirá establecer una medición de la efectividad en las acciones de tratamiento establecidas. Para ello, el dueño del proceso o gestor de riesgo deberá establecer la meta o el valor objetivo del indicador a través del nivel de tolerancia y apetito del riesgo considerado en la política de Gestión Integral del Riesgo aprobada.
El resultado del indicador se debe registrar en la etapa Tratamiento, seguimiento y Revisión - Anexo N° 01; el seguimiento será efectuado por el Gestor del riesgo.

Gráfico N° 08: Indicadores



Fuente: Elaboración OFCR.

En campo Indicador se **debe** describir el Nombre, la Fórmula y la Meta del indicador; en el campo siguiente se **debe** registrar la fecha de medición del riesgo residual.

INDICADOR			FECHA DE MEDICIÓN DEL RIESGO RESIDUAL
NOMBRE DEL INDICADOR DEL RIESGO	FÓRMULA DEL INDICADOR	META DEL INDICADOR	
Porcentaje de DNI entregados a personas distinta al tutular	Cant. Eventos reportados sobre DNI entregados a persona distinta del titular X 100 / Total DNI entregados en la semana	= a 0% Efectivo > 0% y <= 0.01% Parcialmente Efectivo > 0.01% No Efectivo	10/09/2019

La fecha de medición del Indicador **debe** realizarse a los tres meses de haber culminada la implementación de las acciones de tratamiento.

5.5 SEGUIMIENTO Y REVISIÓN

Consiste en la verificación de los planes de gestión del riesgo, para asegurar que las acciones establecidas para el tratamiento de riesgo se están implementando, asimismo, evalúa el cumplimiento y la eficacia en la implementación de acciones para mitigar el riesgo. Pocos riesgos permanecen estáticos, por lo tanto, los riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente para asegurar que circunstancias cambiantes no alteren los objetivos.

Las actividades desarrolladas en esta etapa se encuentran a cargo del Gestor del Riesgo a través del Coordinador del riesgo o Gestor Líder para ello se **debe** realizar lo siguiente:

- ✓ El seguimiento del grado de implementación del Plan de Gestión del Riesgo que incluye la eficacia de los controles y actividades de control establecidos. Así mismo deben analizar los sucesos, incidentes, accidentes, cambios, tendencias, éxitos, errores y fallos que se han producido y detectar los cambios que se puedan producir en el contexto externo – interno que podrían ocasionar cambios en los riesgos, teniendo en cuenta los tratamientos del riesgo implantado y las prioridades establecidas, lo que podría llevar a Identificar nuevos riesgos emergentes.
- ✓ El registro de resultados del Seguimiento y Revisión, para analizar las acciones correctivas y las acciones preventivas.
- ✓ Efectuar la revisión y reporte de forma trimestral del avance del Plan de Gestión del Riesgo al Comité de Control Interno, que incluyen medidas del desempeño (indicadores de riesgo), así como medidas cualitativas y cuantitativas necesarias.
- ✓ Reportar de forma semestral los resultados del Plan de Gestión del Riesgo Ejecutado al Comité de Control Interno.

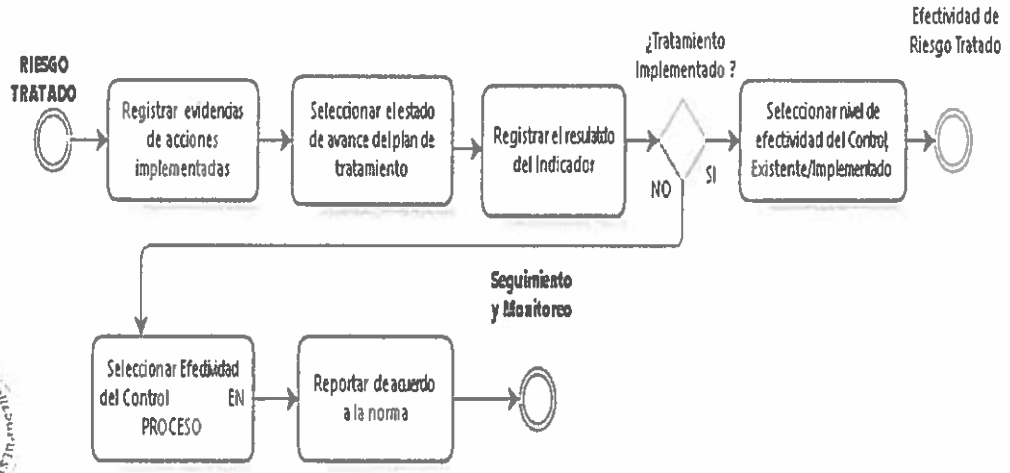
Las actividades que **debe** realizar el Coordinador del riesgo o Gestor Líder y el Equipo de Riesgos en la etapa de Seguimiento y Revisión durante el avance de implementación de las acciones del tratamiento del riesgo en su proceso, serán las siguientes:

N° de Actividad	Descripción de la Actividad
17	Registrar las evidencias que sustentan la implementación de las acciones.
18	Seleccionar el estado de avance del tratamiento, considerando la **Tabla N° 11 Estado de Avance de las acciones Implementadas - Anexo N° 03.**
19	Registrar el resultado del indicador.
20	Seleccionar el nivel de efectividad de acuerdo al resultado del indicador para lo cual **se debe** utilizar la **Tabla N° 12 Nivel de Efectividad del Control Existente/ Implementado - Anexo N° 03.**

Como resultado de estas actividades obtenemos el nivel de efectividad de las acciones del tratamiento que se vienen implementando.

Gráfico N° 09: Seguimiento y Revisión

Estado de avance de implementación de las acciones adoptadas para el Tratamiento del Riesgo - Evaluación del indicador



Fuente: Elaboración OFCR.

Ejemplo: Continuando con el caso, se muestra un modelo con los campos llenados correspondiente a la fecha de medición y el Estado de Avance de la Implementación de las acciones adoptadas para el tratamiento del Riesgo.

ESTADO DE AVANCE DE IMPLEMENTACIÓN DE LAS ACCIONES ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO		EVALUACIÓN DEL INDICADOR	
EVIDENCIAS	ESTADO (TABLA 12)	RESULTADO DEL INDICADOR	NIVEL DE EFECTIVIDAD DEL CONTROL (TABLA 13)
1. 'Plan de Trabajo para la Adquisición de huelleros biométricos a los locales RENIEC. 2. Proyecto de GP-269-GOR/004 "Registros de Trámite y Entrega del Documento Nacional de Identidad" elaborado en revisión por GPP - Memorando N°000152-2018/GOR/RENIEC.	IMPLEMENTADO	0.00%	EN PROCESO DE IMPLEMENTACION

EN PROCESO DE IMPL
EFECTIVO
PARCIALMENTE EFECT
NO EFECTIVO

5.5.1 Cambios y Modificaciones en el Plan de Gestión Integral del Riesgo

Si durante el seguimiento se identifica que las acciones de tratamiento no se vienen implementando de acuerdo a lo planificado o si se han presentado cambios en el entorno interno/externo que generan la variación del tratamiento del riesgo, el Coordinador del riesgo o Gestor Líder a cargo del proceso a través del Gestor del Riesgo **debe** desarrollar las siguientes acciones:

a) Evaluar el estado de avance, analizando los motivos que vienen dificultando el cumplimiento del programa para el tratamiento del riesgo que puedan incluir la identificación nuevos riesgos.
b) Desarrollar gestiones internas a través de comunicaciones y coordinaciones con los responsables, para cumplir con los plazos establecidos en el tratamiento de los riesgos identificados.
c) Reformular el Plan de Gestión del Riesgo, en caso se presenten cambios en las actividades de tratamiento que incluyan mayores periodos de implementación a lo programado o a la incorporación de nuevos riesgos identificados.
d) Reportar al Comité de Control Interno el Plan de Gestión del Riesgo modificado justificando las razones de su variación.

5.5.2 Evaluación del Control Implementado para Obtener el Riesgo Residual

Luego de implementar el tratamiento al riesgo en el periodo programado, se **debe** efectuar la evaluación del control implementado con la finalidad de obtener el RIESGO RESIDUAL; estas actividades permitirán establecer si las acciones implementadas han permitido llevar al riesgo a los niveles establecidos en la Política y Objetivos de la Gestión Integral del Riesgo.

Las actividades que **debe** realizar el Coordinador del riesgo o Gestor Líder y el Equipo de Riesgos en la etapa de Seguimiento y Revisión para obtener el Riesgo residual en su proceso, serán las siguientes:

Nº de Actividad	Descripción de la actividad
21	Realizar las actividades 11 y 12 de la **Etapa Análisis y Valoración del riesgo (Ítem 5.3)**.

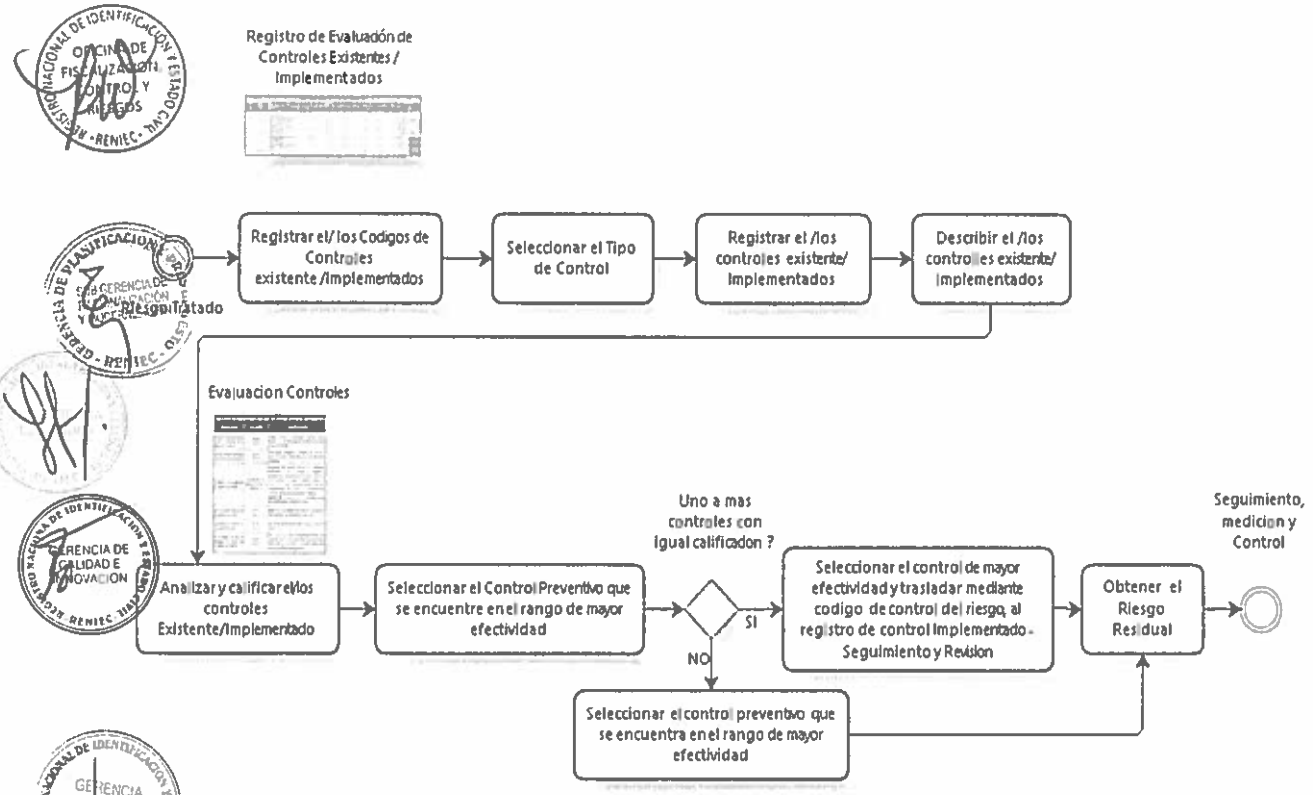
Como resultado de estas actividades obtenemos el Riesgo Residual.

- En el caso que el **Riesgo Residual** resultante no haya permitido llevar al riesgo a los niveles establecidos en la Política y Objetivos de la Gestión Integral del riesgo, el Gestor del Riesgo conjuntamente con el Coordinador del riesgo o Gestor Líder y el equipo de Riesgos **debe** evaluar lo siguiente:

  a. El costo beneficio de adoptar mayores acciones para su tratamiento.
  b. La eficacia y eficiencia de las acciones implementadas.
  c. Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, éste se **debe** mantener en continuo seguimiento y revisión.

  El resultado se **debe** reportar al Comité de Control Interno para su evaluación y toma de decisiones.

Gráfico N° 10: Evaluación de Control o Controles Implementados para obtener el Riesgo Residual



Ejemplo: Continuando con el caso, se muestra un modelo con los campos llenados para la evaluación del control y obtener el Riesgo Residual.

ITEM	CODIGO DEL CONTROL DEL RIESGO	CONTROL EXISTENTE	
		TIPO DE CONTROL EXISTENTE (TABLA 6)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA 7)
5	P08.01.03.03_C005	PREVENTIVO	**Qué:** Homologación y/o validación de imágenes (firma e impresión dactilar) **Cuál:** GP-269-GOR/004 "Registros de Trámite y Entrega del Documento Nacional de Identidad". **Quién:** El registrador de entregas de DNI. **Cómo:** Verificación de las imágenes capturadas versus la información del sistema. **Cuándo:** Permanente en cada entrega de DNI.

SIN CONTROLES
PREVENTIVO
CORRECTIVO

CRITERIOS PARA EL ANALISIS DEL CONTROL EXISTENTE												CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA 8)
¿Existe un medio documentado o vigente y actualizado para la aplicación del control?		¿Se han definido responsable (s) de la ejecución del control?		¿Cuál es el tipo de aplicación de control que se realiza?		¿Se ha definido la frecuencia de aplicación del control?		¿Se cuenta con evidencias de la ejecución y seguimiento del control?		¿En el tiempo que lleva la aplicación del control ha demostrado ser efectiva?			
SI	20	SI	10	SEMIAUTOMATICO	10	SI	10	SI	25	SI	20	95	EFECTIVO

EVALUACIÓN PARA OBTENER EL RIESGO RESIDUAL					
PROBABILIDAD	VALOR	IMPACTO	VALOR	P X I	RIESGO RESIDUAL
MUY IMPROBABLE	1	MODERADO O MEDIO	3	3	TOLERABLE

En el Ejemplo podemos visualizar que luego de la evaluación del control implementado se ha reducido la probabilidad y el impacto, llevando al riesgo residual a un nivel de Riesgo Tolerable.

MATRIZ DE PROBABILIDAD E IMPACTO O MAPA DE CALOR
(PROBABILIDAD x IMPACTO)

PROBABILIDAD							
	Practicamente Seguro	5	TOLERABLE	MODERADO	IMPORTANTE	CRÍTICO	CRÍTICO
	Probable	4	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE	CRÍTICO
	Posible	3	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE
	Improbable	2	ADMISIBLE	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE
	Muy Improbable	1	ADMISIBLE	ADMISIBLE	TOLERABLE	MODERADO	MODERADO
			1	2	3	4	5
			Insignificante o Muy Bajo	Leve o Bajo	Moderado o Medio	Grave o Alto	Catastrófico o Muy alto
			IMPACTO				

5.6 SEGUIMIENTO MEDICIÓN Y CONTROL

Actividad permanente que **debe** efectuar la OFCR, así como los órganos competentes en la Gestión Integral del riesgo en la Entidad, para verificar y evaluar lo siguiente:

- ✓ Los Planes de Gestión del Riesgo formulados por las áreas de la entidad.
- ✓ La implementación de los planes de tratamientos formulados.
- ✓ La eficacia de los resultados reportados.

Para el desarrollo de estas actividades, la OFCR y los órganos competentes en la Gestión Integral del riesgo en la Entidad, recibirán los Planes de Gestión del riesgo remitidos por las áreas a través del Comité de Control Interno. Con la información recibida se **debe** desarrollar las siguientes acciones:

- ✓ Consolidar los planes de Gestión del Riesgo remitidos por las áreas a cargo de los procesos de la entidad.
- ✓ Verificar y evaluar el Plan de Gestión del Riesgo de las áreas que incluyan las todas las etapas, de acuerdo a los criterios formulados en el presente documento.
- ✓ Reportar el resultado de la evaluación de la ejecución de los planes de Gestión del riesgo de las áreas y de ser el caso efectuar recomendaciones a fin que adopten las acciones correctivas necesarias.
- ✓ Formular el Plan de Gestión del Riesgo Institucional, el cual será remitido al Comité de Control Interno para su aprobación y posterior remisión a la Alta Dirección.
- ✓ Efectuar el seguimiento y monitoreo de Plan de Gestión del Riesgo Institucional, reportando los avances al Comité de Control Interno.

Para la revisión de los planes de Gestión Integral del riesgo se **debe** verificar lo siguiente:

- El cumplimiento de los plazos establecidos para la implementación de las acciones formuladas en el plan de tratamiento de los riesgos. identificados.
- El nivel de efectividad de las acciones implementadas.
- La adopción de medidas correctivas en caso se haya presentado dificultades en su proceso de implementación o se haya identificado nuevos riesgos.

✓ Formular el Plan de visitas basada en riesgo de la OFCR para verificar la implementación del plan de gestión del riesgo en las en los procesos de la Entidad.

✓ Reportar al Comité de Control Interno los resultados de la Ejecución de los planes de la Gestión del riesgo de las áreas y el Plan de Gestión del Riesgo Institucional.

Ejemplo: Continuando con el caso, se muestra un modelo con los campos que **debe** registrar la OFCR y según corresponda los órganos técnicos responsables sobre el seguimiento medición y control.

SEGUIMIENTO MEDICION Y CONTROL PARA EL ÁREA EVALUADORA	
ESTADO DEL RIESGO (TABLA 14)	RECOMENDACIONES
MITIGADO	El riesgo ha sido mitigado, pero se recomienda monitoreo permanente mediante el indicador.

5.7 COMUNICACIÓN Y CONSULTA

El propósito de la Comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, es un proceso que fluye de arriba hacia abajo (TOP DOWN) y de abajo hacia arriba (UP DOWN), de manera que se puedan tomar decisiones informadas correctamente mientras que la consulta implica obtener retroalimentación e información para tomar 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.

La entidad dispone de recursos que permiten garantizar la comunicación interna entre todos los niveles de la organización, así como la recepción, documentación y respuesta a las comunicaciones de origen externo. Por lo cual se seguirá lo indicado en la DI-417-SGEN/010 "Gestión Documental del RENIEC".

La comunicación interna para la Gestión Integral del Riesgo se describe a continuación:

Cuadro N° 02: Comunicación Interna (Documentos Normativos)

¿Qué?	¿Cuándo?	¿A quién?	¿Cómo?	¿Quién?
Política y Objetivos de la Gestión Integral del Riesgo y de la Gestión de Riesgos de Seguridad de la Información.	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. Notita informativa Micrositio de Control Interno Inducción a personal nuevo. SITD	GPP/SGRM GII GTH ER
Directiva de 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	GPP/SGRM GG/OFCR
Directivas de Seguridad de la Información.	Cuando se realizan modificaciones a la misma. De forma permanente.	A los funcionarios y servidores de la Entidad.	Intranet. Sensibilización SITD	GPP/SGRM OSDN
Manual de la 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	GPP/SGRM GG/OFCR

Cuadro N° 03: Flujo de Comunicación Interna

¿Qué se debe comunicar?	¿Dónde se genera la información?	¿Quién debe comunicar?	¿A quién?	¿Cómo?	¿Cuándo?	Resultado
Plan de Gestión de Riesgos	Procesos Institucionales	Coord. del Riesgo/ Gestor Líder de la S.I.	Gerente/ Gestor del Riesgo/ Dueño del Riesgo S.I.	SITD	Semestral	Plan de Gestión de Riesgos Aprobada por el Gestor del Riesgo/Gerente/Dueño del Riesgo S.I.
Plan de Gestión de Riesgos Aprobada por el Gestor del Riesgo/Gerente/Dueño del Riesgo	Procesos Institucionales	Gerente/ Gestor del Riesgo/ Dueño del Riesgo S.I.	Secretaría General/ Gerencia General CGSI Cc Pdte. del CCI Cc OFCR Cc OSDN	SITD	Semestral	Informe de Resultados (Mapa de Riesgos institucionales)
Informe de Resultados (Mapa de Riesgos institucionales)	Procesos de Gestión de Riesgos – OFCR / OSDN	Jefe de la OFCR/ Oficial de Seguridad de la Información	CCI Cc Secretaría General Cc Gerencia General Comité de Gestión de Seguridad de la Información (CGSI)	SITD	Semestral	Informe aprobado de resultados de la Gestión de Riesgos Institucional.
Informe aprobado de resultados de la Gestión de Riesgos Institucional	CCI	Pdte. Del CCI.	Jefatura Nacional	SITD	Semestral	Informe aprobado por Jefatura Nacional.

5.8 REGISTRO E INFORME

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

Los Registros utilizados para la Gestión Integral del Riesgo deben ser suscritos y firmados por los responsables que elabora, revisa y aprueba, así mismo, debe registrase la fecha de elaboración y número de versión.

De acuerdo a los cambios en el contexto interno/externo en la Gestión Integral del Riesgo, 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.

5.9 IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN Y TRATAMIENTO DE OPORTUNIDADES

Las oportunidades son situaciones favorables que podrían permitir el logro de un objetivo, 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, tanto de hacer las cosas bien, teniendo en cuenta la situación actual (y sus riesgos), 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, reducir las mermas o mejorar la productividad y mejora de los servicios. Las acciones para abordar las oportunidades también pueden incluir la consideración de los riesgos asociados.

En el tratamiento se **debe** priorizar las oportunidades valoradas como **"Alta"** o **"Muy alta"**, para las oportunidades valoradas como **"Moderada"**, se aplicará el análisis costo-beneficio, de acuerdo a los lineamientos institucionales (**Anexo N° 04**).

Para identificar analizar, valorar y tratar las oportunidades se **debe** utilizar el formato **Plan de Gestión de Oportunidades – Anexo N° 04** y las Tablas contenidas en el **Anexo N° 05.**

VI. VIGENCIA

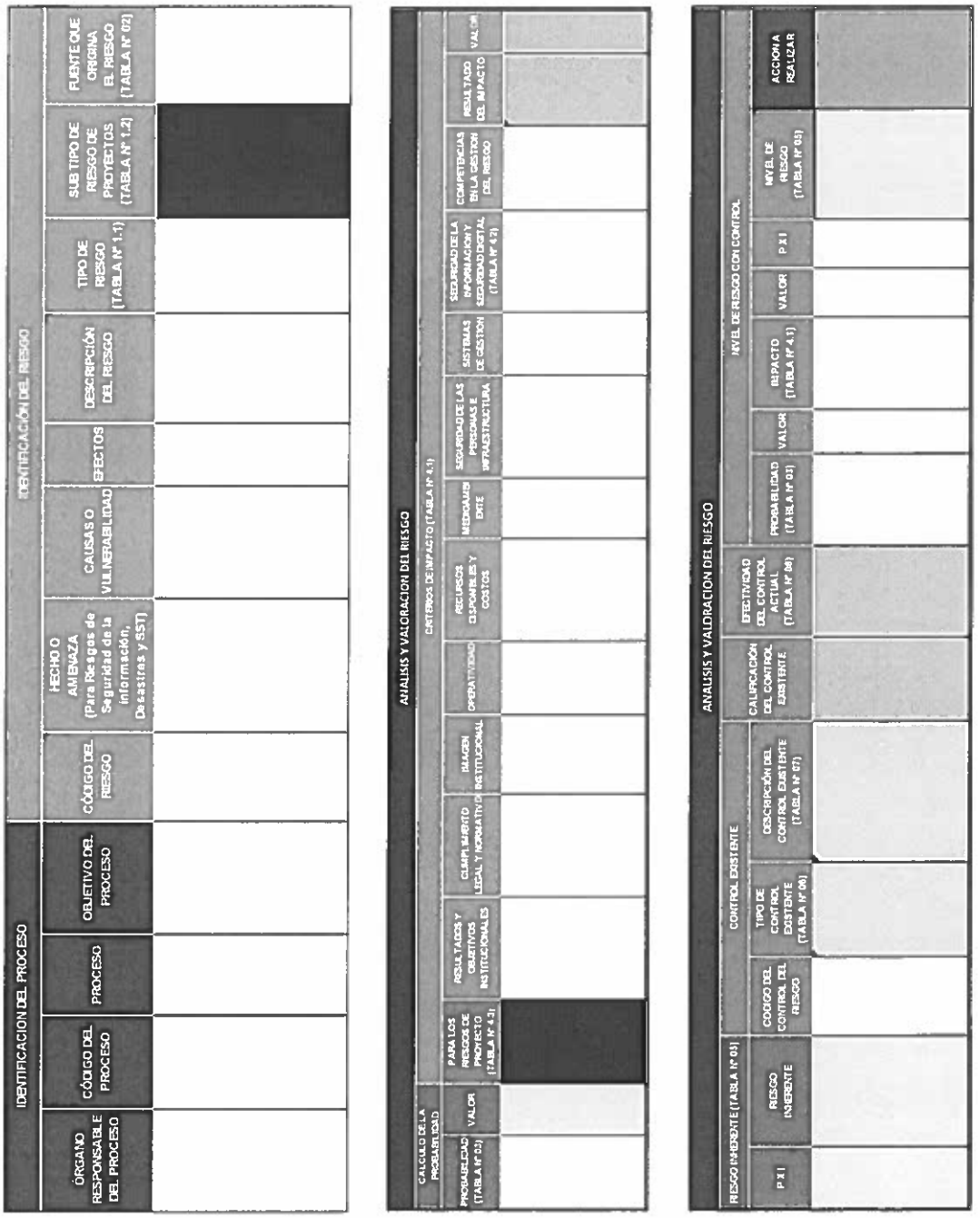
Entrará en vigencia a partir de su aprobación.

VII. APROBACIÓN

Mediante Resolución Secretarial.

VIII. ANEXOS

ANEXO N° 01:
Plan de Gestión Integral del Riesgo



IDENTIFICACION DEL PROCESO				IDENTIFICACIÓN DEL RIESGO								
ÓRGANO RESPONSABLE DEL PROCESO	CÓDIGO DEL PROCESO	PROCESO	OBJETIVO DEL PROCESO	CÓDIGO DEL RIESGO	HECHO O AMENAZA (Para Riesgos de Seguridad de la información, Desastres y SST)	CAUSAS O VULNERABILIDAD	EFECTOS	DESCRIPCIÓN DEL RIESGO	TIPO DE RIESGO (TABLA N° 1.1)	SUB TIPO DE RIESGO DE PROYECTOS (TABLA N° 1.2)	FUENTE QUE ORIGINA EL RIESGO (TABLA N° 02)

ANALISIS Y VALORACION DEL RIESGO																				
CALCULO DE LA PROBABILIDAD		CRITERIOS DE IMPACTO (TABLA N° 4.1)																		
PROBABILIDAD (TABLA N° 03)	VALOR	PARA LOS RIESGOS DE PROYECTO (TABLA N° 4.1)	RESULTADOS Y OBJETIVOS INSTITUCIONALES	CUMPLIMIENTO LEGAL Y NORMATIVO	IMAGEN INSTITUCIONAL	OPERATIVIDAD	RECURSOS DISPONIBLES Y COSTOS	MEDIOAMBIENTE	SEGURIDAD DE LAS PERSONAS E INFRAESTRUCTURA	SISTEMAS DE GESTIÓN	SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL (TABLA N° 4.2)	COMPETENCIAS EN LA GESTIÓN DEL RIESGO	RESULTADO DEL IMPACTO	VALOR

ANALISIS Y VALORACION DEL RIESGO																		
RIESGO INHERENTE (TABLA N° 01)		CONTROL EXISTENTE					NIVEL DE RIESGO CON CONTROL											
P X I	RIESGO INHERENTE	CÓDIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL EXISTENTE (TABLA N° 06)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA N° 07)	CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL ACTUAL (TABLA N° 08)	PROBABILIDAD (TABLA N° 01)	VALOR	IMPACTO (TABLA N° 4.1)	VALOR	P X I	NIVEL DE RIESGO (TABLA N° 03)	ACCIONES A REALIZAR

ANEXO N° 01:
Registro de Análisis del Contexto y Partes Interesadas

ANEXO N° 01

MATRIZ DEL CONTEXTO Y PARTES INTERESADAS - GESTIÓN INTEGRAL DEL RIESGO

MARCO LEGAL	Ley N° 26497, Ley Orgánica del RENIEC de fecha 12 de julio de 1995, fue creado por en concordancia con los artículos 177° y 183° de la Constitución Política del Perú.
MISIÓN	"Registrar la identidad, los hechos vitales y los cambios de estado civil de las personas; participar del sistema electoral y promover el uso de la identificación y certificación digital, con inclusión social y enfoque intercultural".
VISIÓN	"Ciudadanos identificados con acceso a servicios amigables e innovadores en tiempo real, integrados digitalmente a través de la entidad de registro del estado peruano que garantiza su identidad y seguridad jurídica, y que contribuye a la modernización del estado y al desarrollo del país".
NORMATIVA ESPECIFICA (según competencias)[1]	Registro de la identificación, insaurado en el artículo 2° de la Ley Orgánica de creación del RENIEC, el cual está referido a un registro jurídico de carácter público en el que se inscriben las personas naturales y cuyos datos de identificación permite emitir el documento nacional de identidad (DNI), que cumple la función de cedula identificadora y título para el ejercicio de la ciudadanía.
OBJETIVO ESTRATÉGICO INSTITUCIONAL (OEI)[2]	OEI 1: Fortalecer los registros de la identidad y de la identificacion en beneficio de la población.
ACCIONES ESTRATÉGICAS INSTITUCIONALES (AEI)[3]	AEI1.2: Expedición del DNI oportuno para la población
PROCESO (Nivel 0)[4]	P08: Servicio de Atencion al Ciudadano e Institucional
DUEÑO DEL PROCESO (Nivel 0)[5]	Gerencia de Operaciones Registrales
ALCANCE (Nivel 0)[6]	Red de atenciones de la Gerencia de Operaciones Registrales, en el territorio nacional y a traves de las Oficinas Consulares a nivel internacional, que comprende: la atención registral al ciudadano, la gestión operativa de los servicios, el seguimiento y control de los servicios.
PRODUCTOS O SERVICIOS (Nivel 0)[7]	Atención Registral Realizada.

Cod. del proceso[8]	PROCESO[9]	OBJETIVO[10]	ALCANCE[11]	PRODUCTOS / SERVICIOS[12]	REQUISITOS[13]	PARTES INTERESADAS		
						INTERNO[14]	EXTERNO[15]	EXPECTATIVAS[16]
P08.01 ® 3.03	Gestion de entrega de DNI	Brindar servicio de Entrega de DNI.	Comprende desde la recepción de DNI hasta su correspondiente entrega al ciudadano	Sobres de envio de DNI DNI custodados DNI entregado DNI replegado Recaudos custodados	Que Cumpla con la normativa establecida.	Jefatura Regional, Sub Gerencia de Especiales, Sub Gerencia de Aprovisionamiento y Distribucion	Cliente ciudadano, servicios de courier, proveedores, Ministerio de Relaciones Exteriores y entidades publicas y privadas.	Entrega oportuna del DNI y sin errores

LEYENDA:

1 Describir la Normativa específica vinculada a sus competencias, extraer del PEI vigente (Numeral I. CONTEXTO. Incisos a), b), c) y d)), según corresponda o en su defecto referir la Normativa externa a la cual rige su proceso.

2 Registrar el codigo y el nombre de los objetivos estratégicos institucionales (OEI) vinculados a su competencia, establecidos en el PEI vigente (Numeral 4. OBJETIVOS ESTRATEGICOS INSTITUCIONALES. Incisos OEI 1, OEI 2, OEI 3, OEI 4 y OEI 5 segun corresponda.

3 Registrar el codigo y el nombre de las Acciones Estratégicas Institucionales (AEI) asociados a los OEI de su competencia, establecidos en el PEI vigente (Numeral 5 ACCIONES ESTRATEGICAS INSTITUCIONALES. Pagina 21, segun corresponda)

4 Registrar el codigo y nombre del proceso Nivel (0), definido por el Comite de Procesos

5 Registrar el dueño del proceso Nivel (0), definido por el Comite de Procesos

6 Registrar el alcance que comprende el proceso Nivel (0) y las areas involucradas

7 Registrar los productos o servicios que genera el proceso Nivel (0).

8 Registrar el codigo del proceso Nivel (1) definido por el Comite de Procesos

9 Registrar el nombre del proceso Nivel (1)

10 Describir el objetivo del proceso Nivel (1)

11 Describir el alcance que comprende el proceso Nivel (1)

12 Describir los productos o servicios del proceso Nivel (1)

13 Describir los requisitos de los productos o servicios del proceso Nivel (1)

14 Mencionar las partes interesadas internas del proceso Nivel (1)

15 Mencionar las partes interesadas externas del proceso Nivel (1)

16 Describir las expectativas de las partes interesadas internas y/o externas del proceso Nivel (1)

ANEXO N° 01:
Registro para Priorización de Procesos

REGISTRO PARA PRIORIZACIÓN DE PROCESOS

PROCESO INSTITUCIONAL	ÓRGANO	PROCESOS DEL ÓRGANO	ALINEAMIENTO A OBJETIVOS ESTRATÉGICOS INSTITUCIONALES					NIVEL DE CRITICIDAD DEL PROCESO A CARGO DEL ORGANO (PROMEDIO)
			OEI 1	OEI 2	OEI 3	OEI 4	OEI 5	

ANEXO N° 01:
Registro de Evaluación de Controles existentes/implementados

REGISTRO DE EVALUACION DE CONTROLES EXISTENTES / IMPLEMENTADOS											
ITEM	CODIGO DEL CONTROL DEL RIESGO	CONTROL EXISTENTE		CRITERIOS PARA EL ANALISIS DEL CONTROL EXISTENTE						CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA 8)
		TIPO DE CONTROL EXISTENTE (TABLA 6)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA 7)	¿Existe un medio documentado vigente y actualizado para la aplicación del control?	¿Se han definido responsable (s) de la ejecución del control ?	¿Cuál es el tipo de aplicación de control que se realiza?	¿Se ha definido la frecuencia de aplicación del control?	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	¿En el tiempo que lleva la aplicación del control ha demostrado ser efectiva?		
1											

ANEXO N° 02
Técnicas utilizadas en la Gestión del Riesgo

ITEM	HERRAMIENTA	DESCRIPCIÓN
1	Lluvia 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 de 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.

ANEXO N° 03
Tablas para la Gestión Integral del Riesgo

TABLA N° 1.1: TIPOS DE RIESGO

Descripción		Referencia
CORRUPCIÓN	Aquellos relacionados con la 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.	*Decreto Supremo N° 042-2018-PCM (22ABR2018), que establece medidas para fortalecer la integridad pública y lucha contra la corrupción.* *Decreto Supremo N° 044-2018-PCM (26ABR218), que aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021.*
CUMPLIMIENTO	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso social.	*Resolución de Contraloría N° 004-2017-CG (20ENE2017), que aprueba la Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado.*
DESASTRES	Son aquellos asociados a eventos que exponen a la población y sus medios de vida sufran daños y pérdidas como consecuencia de su condición de vulnerabilidad y el impacto de un peligro asociado a fenómenos de origen natural (sismos, tsunamis, actividad volcánica, deslizamientos, aludes, derrumbes y aluviones) o inducidos por la acción humana (incendios, explosiones, contaminación, epidemias, pandemias y otros).	*Ley N° 29664 (19FEB2011) que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).* *Decreto Supremo N° 048-2011-PCM (26MAY2011), que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).*
ESTRATÉGICO	Se asocian con la gobernanza de la entidad. La gestión del riesgo estratégico se enfoca en asuntos globales relacionados con la visión-misión y el cumplimiento de los objetivos institucionales, la clara definición de políticas, el diseño y conceptualización de la entidad por parte de la Alta Dirección.	*Resolución de Contraloría N° 004-2017-CG (20ENE2017), que aprueba la Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado.*
FINANCIERO	Se relacionan con la gestión de los recursos de la entidad con eficiencia y transparencia. Incluye la ejecución presupuestal, la elaboración de los estados financieros, los cobros y pagos, gestión de excedentes de tesorería y la administración de los bienes.	*Resolución de Contraloría N° 004-2017-CG (20ENE2017), que aprueba la Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado.*
IMAGEN	Relacionados con la percepción y la confianza por parte de los grupos de interés en la entidad.	*Elaboración por la OFCR.*
MEDIO AMBIENTE	Comprende aquellos riesgos que pueden ocasionar deterioro o daños al medioambiente.	*Elaboración por la OFCR.*
OPERATIVO	Comprende los riesgos relacionados con deficiencias en los procesos, en la estructura organizacional, en la desarticulación entre dependencias, gestión y desempeño de las personas los cuales conducen a ineficiencias e incumplimiento de los compromisos institucionales.	*Resolución de Contraloría N° 004-2017-CG (20ENE2017), que aprueba la Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado.*
PROYECTOS	Es un evento o condición que, si ocurre, tiene un efecto sobre los objetivos del proyecto (desarrollo normal y previsto). Los riesgos pueden ser positivos o negativos. Los riesgos negativos influyen negativamente sobre alguno o varios objetivos del proyecto, como, por ejemplo: Aumento de los costes del proyecto, retraso del proyecto, disminución de la calidad, impacto en el medio ambiente, pérdida o daños a personas, propiedades o terceros, entre otros.	*Guía de los Fundamentos Para la Dirección de Proyectos (Guía del PMBOK®)–Sexta Edición.*
SEGURIDAD DE LA INFORMACIÓN	Aquellos originados por una amenaza concreta y la posibilidad de explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. El activo es valioso, no solo por su costo, sino también por garantizar la Confidencialidad Integridad y Disponibilidad de la información.	*Glosario – ISO 27000*
TECNOLÓGICO	Comprende los riesgos que afectan al entorno digital. Es decir, al ámbito desarrollado por la TIC´S, dispositivos digitales, internet, tecnologías y dispositivos móviles, la analítica de datos para generar contenido digital; incluyendo el desarrollo de servicios y aplicaciones digitales, en el contexto del gobierno digital.	*Resolución de Contraloría N° 004-2017-CG (20ENE2017), que aprueba la Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado.*

TABLA N° 1.2: CATEGORÍA DE RIESGOS DEL PROYECTO		
CATEGORIA	SUB CATEGORÍA	EJEMPLO
Técnicos	Requisitos	Especificaciones pocos precisas
	Tecnología	Dependencia de "nuevos avances" de poco uso real
	Complejidad	Identificar como interactuará (interfaces)
	Calidad	Incumplimiento de los criterios de calidad de los entregables
	Rendimiento y fiabilidad	Por novedad, imposible estimar velocidad y fiabilidad
Externos	Proveedores o Subcontratistas	Retrasos en envíos o entregas
	Normativa	Un cambio legal puede variar alcance y costes
	Mercado	Competidores pueden adelantarse presentando propuestas similares
	Cliente	Los usuarios podrían cambiar la dirección del proyecto
	Político	Cambios de aspectos políticos que afectan al proyecto
	Climatología	Sólo en algunas regiones, para ciertos tipos de proyecto
Organizacional	Dependencias del proyecto	Tareas críticas del proyecto dependen de la culminación de otros proyectos
	Recursos y Priorización	Otros proyectos podrían afectar la disponibilidad de recursos
	Coordinación y apoyo	Demora o retraso de actividades por falta de apoyo y coordinación
	Personas	Baja moral o relaciones del equipo (clima laboral)
Gestión del proyecto	Estimación	Estimaciones del trabajo y costes son incompletos o parciales
	Planificación	Se desconoce el uso de software de planificación
	Control	Cambios constantes en los criterios para valorar el progreso
	Comunicación	Informes poco claros sobre la evolución del proyecto

TABLA N° 02: FUENTE DEL RIESGO	
INTERNA	Son factores internos que pueden generar riesgos tales como: manejos de recursos, estructura organizacional, disponibilidad presupuestal, procesos, capacidad directiva, capacidad tecnológica, capacidad del talento humano, comunicación organizacional, disponibilidad de la información, infraestructura, continuidad operativa, cultura, imagen, motivación, entre otros.
EXTERNA	Son factores externos que pueden generar riesgos tales como: legales, recortes presupuestales, sociales, tecnológicos, geográficos, ambientales entre otros.

TABLA N° 03: PROBABILIDAD		
Clasificación	**Nivel**	**Descripción y Frecuencia**
Muy Improbable	1	El riesgo podría ocurrir rara vez, sólo en circunstancias excepcionales en un horizonte aproximado mayor a un año.
Improbable	2	El riesgo podría materializarse en algún momento u ocasionalmente en un horizonte aproximado de un año.
Posible	3	El riesgo puede ocurrir en algún momento; relativamente frecuente en un futuro cercano menor a un semestre.
Probable	4	El riesgo puede ocurrir en la mayoría de las circunstancias. Aproximadamente una vez al mes.
Prácticamente Seguro	5	Se espera que el riesgo ocurra en la mayoría de las circunstancias; en un presente muy cercano. Aproximadamente en días o semanas

Nota importante:
El análisis de la probalidad 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, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

TABLA N° 4.1: IMPACTO PARA RIESGOS EN GENERAL

Impacto	Nivel	Resultados y Objetivos Institucionales	Cumplimiento legal y normativo	Imagen Institucional	Operatividad	Recursos disponibles y costos
INSIGNIFICANTE O MUY BAJO	1	No hay consecuencias o sus efectos son insignificantes en los resultados y objetivos 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, pero si por el cliente interno.	No se interrumpe la operatividad. Las consecuencias pueden ser asimiladas en las actividades del proceso.	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daños insignificantes o inexistentes.
LEVE O BAJO	2	Consecuencias mínimas en los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto leve. No hay penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias leves que son percibidas por el cliente ciudadano y el cliente interno. Afecta mínimamente la imagen institucional.	Mínimas interrupciones en la operatividad, las consecuencias son asimiladas en las actividades del proceso.	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daño y su recuperación son mínimos.
MODERADO O MEDIO	3	Consecuencias afectan medianamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto moderado. Hay penalidades, multas o sanciones menores, observaciones-recomendaciones de auditorías, o similares.	Consecuencias son percibidas por el cliente ciudadano, el cliente interno y otros grupos de interés, afectan a la imagen institucional. Se originan quejas, reclamos, denuncias o similares.	Existen interrupciones en la operatividad y las consecuencias pueden afectar al proceso o a sus principales actividades deteriorando su productividad.	Las consecuencias demandarán mayores recursos. Los costos del daño y su recuperación son moderados.
GRAVE O ALTO	4	Consecuencias afectan significativamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto grave. Hay fuertes penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan significativamente a la imagen de la entidad, son percibidas por los grupos de interés. Se originan graves quejas, reclamos, denuncias o similares.	Interrupción parcial de la operatividad afectando a varios procesos de la institución.	Las consecuencias demandarán mayores recursos disponibles. El costo del daño y su recuperación es importante, requiere ajustes presupuestales.
CATASTRÓFICO O MUY ALTO	5	Consecuencias afectan catastróficamente los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto catastrófico. Hay graves multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan de manera catastrófica deteriorando la imagen institucional ante los grupos de interés. Se originan muy graves quejas, reclamos, denuncias o similares.	Interrupción total de la operatividad de la institución.	Requiere recursos extraordinarios. El costo de la pérdida y su recuperación es muy alto, requerirá presupuesto adicional significativo.

Impacto	Nivel	Medioambiente	Sistemas de Gestión de la Calidad y otros	Competencias en la Gestión del Riesgo
INSIGNIFICANTE O MUY BAJO	1	Poca o nula afectación al medioambiente. Posibilita una recuperación inmediata de las condiciones originales tras el cese de la acción. Afecta únicamente el área de trabajo.	Las consecuencias no afectan a los Sistemas de Gestión.	El personal cuenta con las competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
LEVE O BAJO	2	Baja alteración en el medioambiente. Posibilita una pronta recuperación de las condiciones originales tras el cese de la acción. La afectación sale del área de trabajo, pero se mantiene bajo el control institucional.	Las consecuencias generan oportunidades de mejora a los Sistemas de Gestión.	El personal reúne las principales competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
MODERADO O MEDIO	3	Media alteración en el medioambiente. Posibilita una recuperación en el mediano plazo de las condiciones originales tras el cese de la acción. Afecta levemente a terceros.	Las consecuencias generan observaciones de fácil atención, no afectan a los Sistemas de Gestión.	El personal cuenta parcialmente con las competencias requeridas y tiene conocimiento parcial de los riesgos inherentes a su actividad.
GRAVE O ALTO	4	Alta alteración en el medioambiente. Recuperación solo en el largo plazo de las condiciones originales tras el cese de la acción. Afecta en mayor grado a terceros.	Las consecuencias generan no conformidades menores, no afectan a los Sistemas de Gestión.	Las competencias que requiere el personal están desactualizadas y carece de conocimientos de los riesgos.
CATASTRÓFICO O MUY ALTO	5	Grave afectación al medioambiente. Perdida permanente en la calidad de las condiciones y recursos ambientales sin posibilidad de recuperación. Afecta gravemente a terceros.	Las consecuencias generan no conformidades mayores afectando a los Sistemas de Gestión. Pérdida de la certificación.	El personal no cuenta con las competencias ni conocimientos requeridos.

TABLA N° 4.2: IMPACTO PARA RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

Impacto	Nivel	Seguridad de la Información y Seguridad Digital	Resultados y Objetivos Institucionales	Cumplimiento legal y normativo	Imagen Institucional	Operatividad
INSIGNIFICANTE O MUY BAJO	1	Las consecuencias no afectan la Confidencialidad, Integridad y Disponibilidad de la información. No se afecta el entorno digital o físico donde se genera, almacena o distribuye la información.	No hay consecuencias o sus efectos son insignificantes en los resultados y objetivos 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, pero si por el cliente interno.	No se interrumpe la operatividad. Las consecuencias pueden ser asimiladas en las actividades del proceso.
LEVE O BAJO	2	Las consecuencias afectan levemente la Confidencialidad, Integridad o Disponibilidad de la información. La afectación del entorno digital o físico donde se genera, almacena o distribuye la información es mínima y recuperable.	Consecuencias mínimas en los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto leve. No hay penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias leves que son percibidas por el cliente ciudadano y el cliente interno. Afecta mínimamente la imagen institucional.	Mínimas interrupciones en la operatividad, las consecuencias son asimiladas en las actividades del proceso.
MODERADO O MEDIO	3	Las consecuencias afectan moderadamente la Confidencialidad, Integridad o Disponibilidad de la información. La afectación del entorno digital o físico donde se genera, almacena o distribuye la información es moderada sin pérdida de información, su recuperación demanda recursos adicionales.	Consecuencias afectan medianamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto moderado. Hay penalidades, multas o sanciones menores, observaciones-recomendaciones de auditorías, o similares.	Consecuencias son percibidas por el cliente ciudadano, el cliente interno y otros grupos de interés, afectan a la imagen institucional. Se originan quejas, reclamos, denuncias o similares.	Existen interrupciones en la operatividad y las consecuencias pueden afectar al proceso o a sus principales actividades deteriorando su productividad.
GRAVE O ALTO	4	Las consecuencias afectan gravemente la Confidencialidad, Integridad o Disponibilidad de la información. La afectación del entorno digital o físico donde se genera, almacena o distribuye la información es grave con pérdida parcial de información, perjudicando la toma de decisiones.	Consecuencias afectan significativamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto grave. Hay fuertes penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan significativamente a la imagen de la entidad, son percibidas por los grupos de interés. Se originan graves quejas, reclamos, denuncias o similares.	Interrupción parcial de la operatividad afectando a varios procesos de la institución.
CATASTRÓFICO O MUY ALTO	5	Las consecuencias afectan de manera crítica la Confidencialidad, Integridad o Disponibilidad de la información. La afectación del entorno digital o físico donde se genera, almacena o distribuye la información es muy grave con pérdida total de la información.	Consecuencias afectan catastróficamente los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto catastrófico. Hay graves multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan de manera catastrófica deteriorando la imagen institucional ante los grupos de interés. Se originan muy graves quejas, reclamos, denuncias o similares.	Interrupción total de la operatividad de la institución.

Impacto	Nivel	Recursos disponibles y costos	Medioambiente	Sistemas de Gestión de la Calidad y otros	Competencias en la Gestión del Riesgo
INSIGNIFICANTE O MUY BAJO	1	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daños insignificantes o inexistentes.	Poca o nula afectación al medioambiente. Posibilita una recuperación inmediata de las condiciones originales tras el cese de la acción. Afecta únicamente el área de trabajo.	Las consecuencias no afectan a los Sistemas de Gestión.	El personal cuenta con las competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
LEVE O BAJO	2	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daño y su recuperación son mínimos.	Baja alteración en el medioambiente. Posibilita una pronta recuperación de las condiciones originales tras el cese de la acción. La afectación sale del área de trabajo, pero se mantiene bajo el control institucional.	Las consecuencias generan oportunidades de mejora a los Sistemas de Gestión.	El personal reúne las principales competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
MODERADO O MEDIO	3	Las consecuencias demandarán mayores recursos. Los costos del daño y su recuperación son moderados.	Media alteración en el medioambiente. Posibilita una recuperación en el mediano plazo de las condiciones originales tras el cese de la acción. Afecta levemente a terceros.	Las consecuencias generan observaciones de fácil atención, no afectan a los Sistemas de Gestión.	El personal cuenta parcialmente con las competencias requeridas y tiene conocimiento parcial de los riesgos inherentes a su actividad.
GRAVE O ALTO	4	Las consecuencias demandarán mayores recursos disponibles. El costo del daño y su recuperación es importante, requiere ajustes presupuestales.	Alta alteración en el medioambiente. Recuperación solo en el largo plazo de las condiciones originales tras el cese de la acción. Afecta en mayor grado a terceros.	Las consecuencias generan no conformidades menores, no afectan a los Sistemas de Gestión.	Las competencias que requiere el personal están desactualizadas y carece de conocimientos de los riesgos.
CATASTRÓFICO O MUY ALTO	5	Requiere recursos extraordinarios. El costo de la pérdida y su recuperación es muy alto, requerirá presupuesto adicional significativo.	Grave afectación al medioambiente. Perdida permanente en la calidad de las condiciones y recursos ambientales sin posibilidad de recuperación. Afecta gravemente a terceros.	Las consecuencias generan no conformidades mayores afectando a los Sistemas de Gestión. Pérdida de la certificación.	El personal no cuenta con las competencias ni conocimientos requeridos.

TABLA N° 4.3: IMPACTO PARA RIESGO DE PROYECTOS					
Impacto	Nivel	Impactos para Riesgos de Proyectos	Resultados y Objetivos Institucionales	Cumplimiento legal y normativo	Imagen institucional
INSIGNIFICANTE O MUY BAJO	1	Alcance: Disminución del alcance muy baja, apenas perceptible. Tiempo: Menos del 5% de retraso. Costo: menos del 5% de sobrecosto Calidad: Ningún cambio en la funcionalidad.	No hay consecuencias o sus efectos son insignificantes en los resultados y objetivos 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, pero sí por el cliente interno.
LEVE O BAJO	2	Alcance: Disminución del alcance baja o requerimientos. Tiempo: Entre 5 y 10% de retraso. Costo: Entre 5 y 10% de sobrecosto. Calidad: Impacto menor sobre la funcionalidad general.	Consecuencias mínimas en los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto leve. No hay penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias leves que son percibidas por el cliente ciudadano y el cliente interno. Afecta mínimamente la imagen institucional.
MODERADO O MEDIO	3	Alcance: incumplimiento de requisitos importantes Tiempo: entre 10 y 15 % de retraso Costo: entre 10 y 15 % de sobrecosto Calidad: Algún impacto sobre áreas funcionales clave	Consecuencias afectan medianamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto moderado. Hay penalidades, multas o sanciones menores, observaciones-recomendaciones de auditorías, o similares.	Consecuencias son percibidas por el cliente ciudadano, el cliente interno y otros grupos de interés, afectan a la imagen institucional. Se originan quejas, reclamos, denuncias o similares.
GRAVE O ALTO	4	Alcance: Reducción del alcance inaceptable para el patrocinador Tiempo: entre 15 y 20% de retraso Costo: entre 15 y 20% de sobrecosto Calidad: Impacto significativo sobre la funcionalidad general	Consecuencias afectan significativamente a los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto grave. Hay fuertes penalidades, multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan significativamente a la imagen de la entidad, son percibidas por los grupos de interés. Se originan graves quejas, reclamos, denuncias o similares.
CATASTRÓFICO O MUY ALTO	5	Alcance: No cumple con los requisitos Tiempo: + 20% Retraso Costo: + 20% sobrecosto Calidad: Impacto muy significativo sobre la funcionalidad general	Consecuencias afectan catastróficamente los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto catastrófico. Hay graves multas o sanciones, observaciones-recomendaciones de auditorías, o similares.	Consecuencias afectan de manera catastrófica deteriorando la imagen institucional ante los grupos de interés. Se originan muy graves quejas, reclamos, denuncias o similares.

Impacto	Nivel	Operatividad	Recursos disponibles y costos	Medioambiente
INSIGNIFICANTE O MUY BAJO	1	No se interrumpe la operatividad. Las consecuencias pueden ser asimiladas en las actividades del proceso.	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daños insignificantes o inexistentes.	Poca o nula afectación al medioambiente. Posibilita una recuperación inmediata de las condiciones originales tras el cese de la acción. Afecta únicamente el área de trabajo.
LEVE O BAJO	2	Mínimas interrupciones en la operatividad, las consecuencias son asimiladas en las actividades del proceso.	Las consecuencias podrán ser atendidas con los recursos disponibles. Costos de daño y su recuperación son mínimos.	Baja alteración en el medioambiente. Posibilita una pronta recuperación de las condiciones originales tras el cese de la acción. La afectación sale del área de trabajo, pero se mantiene bajo el control institucional.
MODERADO O MEDIO	3	Existen interrupciones en la operatividad y las consecuencias pueden afectar al proceso o a sus principales actividades deteriorando su productividad.	Las consecuencias demandarán mayores recursos. Los costos del daño y su recuperación son moderados.	Media alteración en el medioambiente. Posibilita una recuperación en el mediano plazo de las condiciones originales tras el cese de la acción. Afecta levemente a terceros.
GRAVE O ALTO	4	Interrupción parcial de la operatividad afectando a varios procesos de la institución.	Las consecuencias demandarán mayores recursos disponibles. El costo del daño y su recuperación es importante, requiere ajustes presupuestales.	Alta alteración en el medioambiente. Recuperación solo en el largo plazo de las condiciones originales tras el cese de la acción. Afecta en mayor grado a terceros.
CATASTRÓFICO O MUY ALTO	5	Interrupción total de la operatividad de la institución.	Requiere recursos extraordinarios. El costo de la pérdida y su recuperación es muy alto, requerirá presupuesto adicional significativo.	Grave afectación al medioambiente. Perdida permanente en la calidad de las condiciones y recursos ambientales sin posibilidad de recuperación. Afecta gravemente a terceros.

Impacto	Nivel	Sistemas de Gestión de la Calidad y otros	Competencias en la Gestión del Riesgo
INSIGNIFICANTE O MUY BAJO	1	Las consecuencias no afectan a los Sistemas de Gestión.	El personal cuenta con las competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
LEVE O BAJO	2	Las consecuencias generan oportunidades de mejora a los Sistemas de Gestión.	El personal reúne las principales competencias requeridas y tiene conocimiento de los riesgos inherentes a su actividad.
MODERADO O MEDIO	3	Las consecuencias generan observaciones de fácil atención, no afectan a los Sistemas de Gestión.	El personal cuenta parcialmente con las competencias requeridas y tiene conocimiento parcial de los riesgos inherentes a su actividad.
GRAVE O ALTO	4	Las consecuencias generan no conformidades menores, no afectan a los Sistemas de Gestión.	Las competencias que requiere el personal están desactualizadas y carece de conocimientos de los riesgos.
CATASTRÓFICO O MUY ALTO	5	Las consecuencias generan no conformidades mayores afectando a los Sistemas de Gestión. Pérdida de la certificación.	El personal no cuenta con las competencias ni conocimientos requeridos.

TABLA Nº 05: MATRIZ DE PROBABILIDAD E IMPACTO O MAPA DE CALOR
(PROBABILIDAD x IMPACTO)

PROBABILIDAD						IMPACTO				
Practicamente Seguro	5	TOLERABLE	MODERADO	IMPORTANTE	CRÍTICO	CRÍTICO	1	2	3	4	5
Probable	4	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE	CRÍTICO	Insignificante o Muy Bajo	Leve o Bajo	Moderado o Medio	Grave o Alto	Catastrófico o Muy alto
Posible	3	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE	IMPORTANTE					
Improbable	2	ADMISIBLE	TOLERABLE	TOLERABLE	MODERADO	IMPORTANTE					
Muy Improbable	1	ADMISIBLE	ADMISIBLE	TOLERABLE	MODERADO	MODERADO					

TABLA N° 06: TIPOS DE CONTROL EXISTENTE / IMPLEMENTADO		
PREVENTIVO	Evitan que un evento suceda. **Dentro de esta categoría de controles pueden existir controles de tipo detectivo**, los cuales permiten registrar un evento después de que éste ha sucedido.	- Por ejemplo, el requerimiento de un login y password en un sistema de información es un control preventivo.
CORRECTIVO	No prevén que un evento suceda, pero permiten enfrentar la situación una vez se haya presentado.	- En caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, es posible volver a recuperar las operaciones.
SIN CONTROLES	Que no cuenta con controles.	---

TABLA N° 07: CRITERIOS PARA EL ANÁLISIS DEL CONTROL EXISTENTE / IMPLEMENTADO		
PREGUNTAS	**VALORES**	**JUSTIFICACIÓN**
¿Existe un medio documentado vigente y actualizado para la aplicación del control?	SI = 20 NO = 0	Políticas, Directivas, Lineamientos, Manuales, Guías, Instructivos u otros DDNN vigente y actualizada (De acuerdo a la DI -200/GPP/002).
¿Se han definido responsable (s) de la ejecución del control?	SI = 10 NO = 0	Responsables designados formalmente para ejecutar la acción de control y seguimiento y, a su vez debidamente capacitados.
¿Cuál es el tipo de aplicación de control que se realiza?	AUTOMATICO = 15 SEMIAUTOMATICO = 10 MANUAL = 5	**Automático (A):** Sistemas o Software que permitan incluir contraseñas de acceso o controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de estos, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. **Semiautomático (S):** Actividad que es desarrollada por una persona con ayuda de sistemas informatizados. **Manual (M):** Actividad que es desarrollada por una persona sin ayuda de sistemas informáticos.
¿Se ha definido la frecuencia de aplicación del control?	SI = 10 NO = 0	Periodicidad en la aplicación del control: en cada operación, diario, semanal, mensual, trimestral, anual u otro.
¿Se cuenta con evidencias de la ejecución del control?	SI = 25 NO = 0	Documentos que evidencien la aplicación de las acciones de control.
En el tiempo que lleva la aplicación del control ¿ha demostrado ser efectiva?	SI = 20 NO = 0	Las acciones de control existentes/implementadas para mitigar el riesgo, en este punto deben estar directamente relacionadas con un indicador que demuestre la efectividad del control (cuando la respuesta es SI).

TABLA N° 08: RANGOS DEL RESULTADO DE LA CALIFICACIÓN DEL CONTROL EXISTENTE / IMPLEMENTADO					
Rangos	**Nivel a disminuir**	**Tipo de Control**	**Acción del tipo de control**	**Efectividad del Control**	**Descripción de la efectividad del Control**
Entre 0-50	0	Preventivo Correctivo	Se mantiene el riesgo.	No efectivo	El control implementado no ha cumplido con la meta. No se encuentra dentro del límite de tolerancia del riesgo o se encuentra sobre el nivel de capacidad del riesgo.
Entre 51-75	1	Preventivo	Si el Control es Preventivo la Probabilidad disminuye en un nivel.	Parcialmente efectivo	El control implementado se encuentra en el margen de tolerancia e indica que hay una aproximación al logro de la meta.
		Correctivo	Si el Control es Correctivo el Impacto disminuye en un nivel.		
Entre 76-100	2	Preventivo	Si el Control es Preventivo la Probabilidad disminuye en dos niveles.	Efectivo	El control implementado ha cumplido con la meta, se encuentra dentro del apetito del riesgo (política) o en los límites de tolerancia del riesgo determinados por el gestor del riesgo.
		Correctivo	Si el Control es Correctivo el Impacto disminuye en dos niveles.		

TABLA N° 09: RESPUESTA AL RIESGO	
EVITAR	Implica tomar las medidas para prevenir un riesgo adverso. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación como resultado de la implantación de adecuados controles y acciones emprendidas. Un ejemplo puede ser realizar una reingeniería de los procesos.
REDUCIR	Implica reducir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
COMPARTIR	Consiste en trasladar el impacto negativo de una amenaza, junto con la propiedad de la respuesta, a un tercero. Transferir el riesgo simplemente da a otra parte la responsabilidad de su gestión; no lo elimina. Como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un sólo lugar.
ACEPTAR	Considerando el nivel de riesgo aceptado por la entidad; no se realiza acciones para reducir la probabilidad o el impacto o también se puede aceptar el riesgo a fin de perseguir una oportunidad.

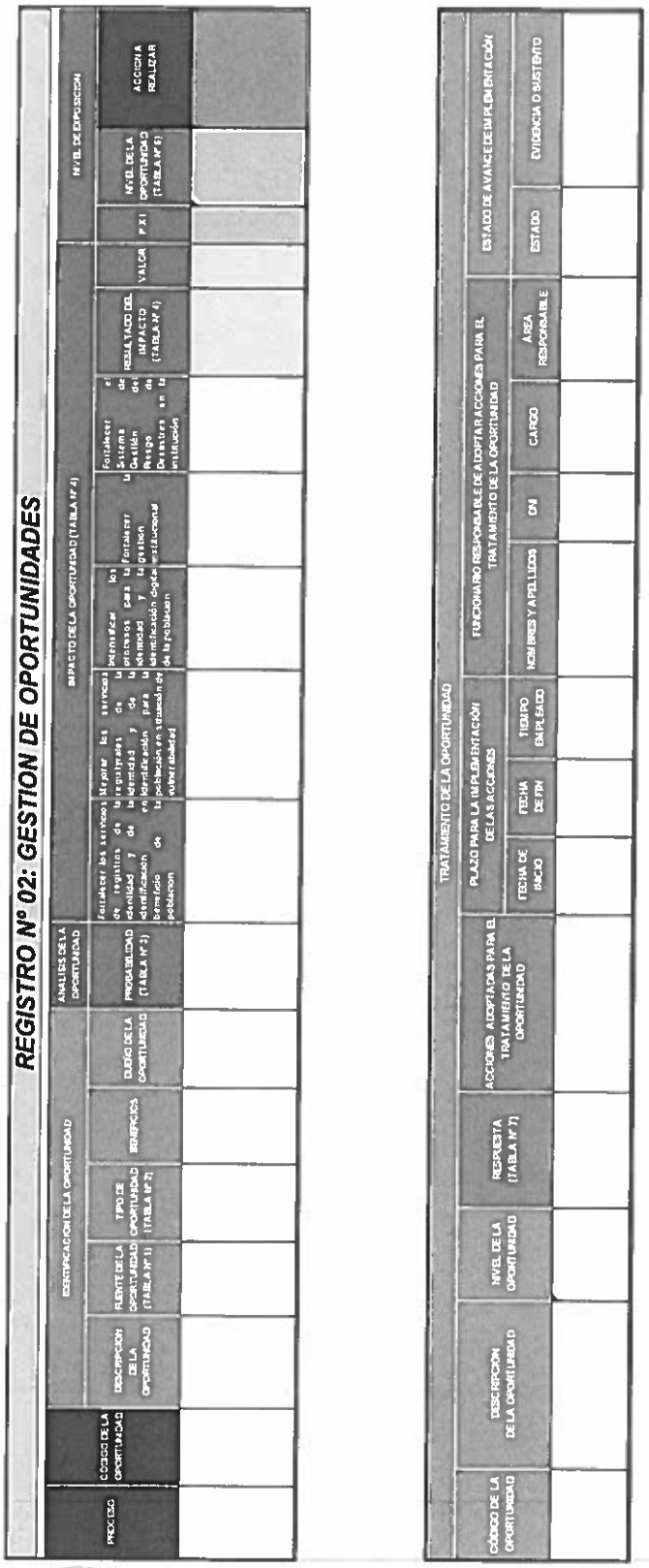
TABLA N° 10 CRITERIOS PARA LA RESPUESTA AL RIESGO EN LA ETAPA DE TRATAMIENTO		
Nivel de exposición	Respuestas	Criterio
Crítico	Evitar, Reducir o Compartir	Los riesgos de nivel Crítico tienen los valores más altos de probabilidad e impacto, requieren de una gestión prioritaria y de una respuesta al riesgo planificada. Deben contar con el Plan de tratamiento, que incluya el Plan de contingencia u otro plan similar, con las aprobaciones correspondientes, para garantizar la oportuna recuperación ante la ocurrencia del riesgo. Se deben aplicar actividades de control y controles adecuados. Deberán reportarse a la Alta Dirección.
Importante	Evitar, Reducir o Compartir	Los riesgos de nivel Importante tienen valores relativamente altos de probabilidad e impacto por lo tanto también deben tener una gestión prioritaria y una respuesta planificada. Requieren Planes de tratamiento del riesgo que incluyan la elaboración de Plan de contingencia con las debidas aprobaciones. Se deben aplicar actividades de control y controles adecuados; se reportan a Alta Dirección.
Moderado	Reducir o Compartir	Los riesgos de nivel moderado se tratan con medidas de control para llevarlos a la zona de riesgos aceptados que comprende los riesgos de nivel Admisible y Tolerable, se aplican acciones preventivas y/o correctivas según corresponda, teniendo en cuenta la relación beneficio/costo del tratamiento.
Tolerable	Aceptar	Para los niveles del riesgo Admisible y Tolerable se aceptarán los riesgos por encontrarse comprendidos en el riesgo aceptado por la entidad, se pueden 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 con procedimientos rutinarios para garantizar que el nivel del riesgo residual se mantiene bajo control.
Admisible		

TABLA N° 11: ESTADO DE AVANCE DE IMPLEMENTACIÓN	
PENDIENTE	Sin acciones para mitigar el riesgo.
EN PROCESO	Las acciones se encuentran en proceso de desarrollo.
IMPLEMENTADO	Las acciones han sido implementadas.

TABLA N° 12: NIVEL DE EFECTIVIDAD DEL CONTROL IMPLEMENTADO	
En proceso de implementación	Cuando las acciones de tratamiento para implementar el control se encuentran en proceso
No efectivo/Inefectivo	El control implementado no ha cumplido con la meta. No se encuentra dentro del límite de tolerancia del riesgo o se encuentra sobre el nivel de capacidad del riesgo.
Parcialmente efectivo/con deficiencias	El control implementado se encuentra en el margen de tolerancia e indica que hay una aproximación al logro de la meta.
Efectivo	El control implementado ha cumplido con la meta, se encuentra dentro del apetito del riesgo (política) o en los límites de tolerancia del riesgo determinados por el gestor del riesgo.

TABLA N° 13: ESTADO DE RIESGO	
MITIGADO	Cuando las acciones adoptadas se reducen, evitan o comparten.
ACEPTADO	Cuando se asume el riesgo al considerar que la probabilidad de ocurrencia e impacto es baja.
SIN ACCIONES	Cuando no se gestiona el riesgo.

ANEXO N° 04
Plan de Gestión de Oportunidades



REGISTRO N° 02: GESTION DE OPORTUNIDADES

PROCESO	IDENTIFICACIÓN DE LA OPORTUNIDAD						ANALISIS DE LA OPORTUNIDAD		IMPACTO DE LA OPORTUNIDAD (TABLA N° 4)											NIVEL DE EXPOSICION		
	CODIGO DE LA OPORTUNIDAD	DESCRIPCION DE LA OPORTUNIDAD	FUENTE DE LA OPORTUNIDAD (TABLA N° 1)	TIPO DE OPORTUNIDAD (TABLA N° 2)	BENEFICIOS	DUEÑO DE LA OPORTUNIDAD	PROBABILIDAD (TABLA N° 3)	Fortalecer los servicios de registros de identidad y de identificación en el domicilio de la población	Reportar las estadísticas de registros de identidad y de identificación para la población en situación de vulnerabilidad	Determinar los procesos para la identificación digital de la población	Fortalecer la gestión	Fortalecer el Sistema de Gestión de Riesgo de Desastres en la institución	RESULTADO DEL IMPACTO (TABLA N° 4)	VALOR	P.XI	NIVEL DE LA OPORTUNIDAD (TABLA N° 5)	ACCIONA REALIZAR

TRATAMIENTO DE LA OPORTUNIDAD

CÓDIGO DE LA OPORTUNIDAD	DESCRIPCIÓN DE LA OPORTUNIDAD	NIVEL DE LA OPORTUNIDAD	RESPUESTA (TABLA N° 7)	ACCIONES ADOPTADAS PARA EL TRATAMIENTO DE LA OPORTUNIDAD	PLAZO PARA LA IMPLEMENTACIÓN DE LAS ACCIONES		FUNCIONARIO RESPONSABLE DE ADOPTAR ACCIONES PARA EL TRATAMIENTO DE LA OPORTUNIDAD			ESTADO DE AVANCE DE IMPLEMENTACIÓN		
					FECHA DE INICIO	FECHA DE FIN	TIEMPO EMPLEADO	NOMBRES Y APELLIDOS	DNI	CARGO	ÁREA RESPONSABLE	ESTADO	EVIDENCIA O SUSTENTO

ANEXO N° 05
Tablas para la Gestión de Oportunidades

TABLA N° 01: FUENTE DE OPORTUNIDAD
INTERNA
EXTERNA

TABLA N° 02: TIPO DE OPORTUNIDAD
SERVICIOS
LEGALES
PERSONAS
TECNOLÓGICAS
GESTIÓN

TABLA N° 03: PROBABILIDAD DE LA OPORTUNIDAD		
Clasificación	Nivel	Oportunidad
PRÁCTICAMENTE SEGURO	5	La ocurrencia es inminente.
PROBABLE	4	**Probablemente se realice**. Se puede dar en el corto plazo.
POSIBLE	3	**Puede ocurrir su realización**. Existen condiciones que probabilidad de realización sea en el mediano plazo.
IMPROBABLE	2	**Podría realizarse** Existen condiciones que hacen que su probabilidad de realización sea a largo plazo.
MUY IMPROBABLE	1	La probabilidad que se pueda realizar es nula.

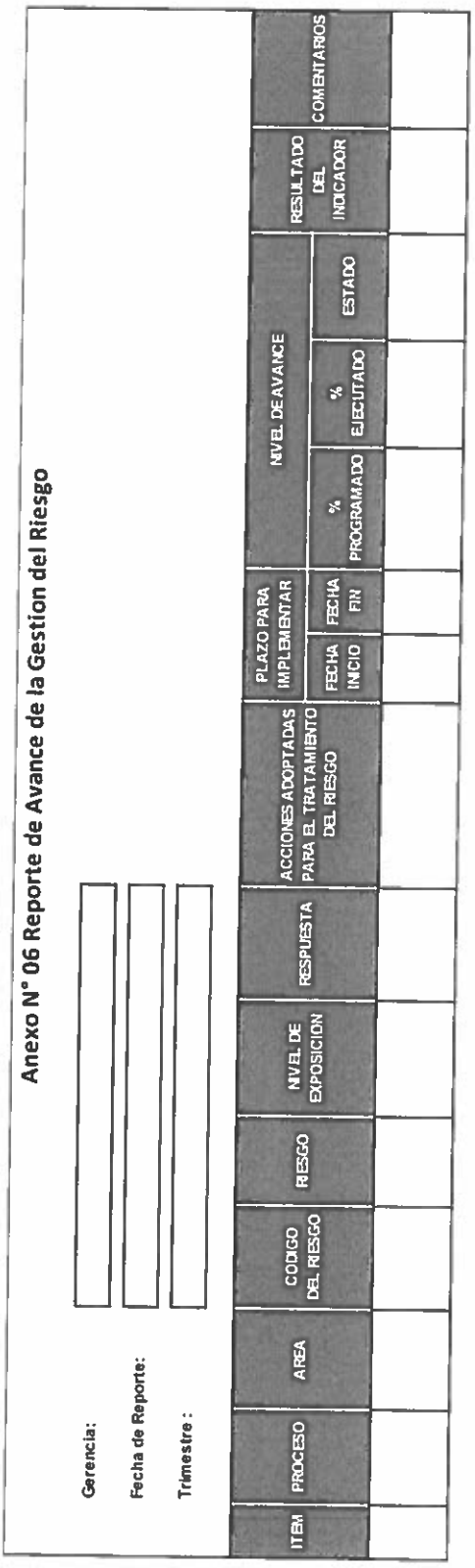
TABLA Nº 04: CRITERIOS DE EVALUACIÓN DE OPORTUNIDADES						
CLASIFICACIÓN	NIVEL	Fortalecer los servicios de registros de la identidad y de la identificación en beneficio de la población	Mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad	Intensificar los procesos para la identidad y la identificación digital de la población	Fortalecer la gestión institucional	Fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución
MUY BAJO	1	La oportunidad no tiene impacto en los servicios de registros de la identidad y de la identificación en beneficio de la población.	La oportunidad no tiene impacto en mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad.	La oportunidad no tiene impacto en Intensificar los procesos para la identidad y la identificación digital de la población.	La oportunidad no tiene impacto en fortalecer la gestión institucional.	La oportunidad no tiene impacto en fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución.
BAJO	2	La oportunidad tiene impacto indirecto, en los servicios de registros de la identidad y de la identificación en beneficio de la población.	La oportunidad tiene impacto indirecto en mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad.	La oportunidad tiene impacto indirecto en Intensificar los procesos para la identidad y la identificación digital de la población.	La oportunidad tiene impacto indirecto en fortalecer la gestión institucional.	La oportunidad tiene impacto indirecto en fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución.
MODERADO	3	La oportunidad tiene impacto directo, en los servicios de registros de la identidad y de la identificación en beneficio de la población y el efecto es moderado.	La oportunidad tiene impacto directo en mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad y el efecto es moderado.	La oportunidad tiene impacto directo en Intensificar los procesos para la identidad y la identificación digital de la población y el efecto es moderado.	La oportunidad tiene impacto directo en fortalecer la gestión institucional y el efecto es moderado.	La oportunidad tiene impacto directo en fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución y el efecto es moderado.
ALTO	4	La oportunidad tiene impacto directo, en los servicios de registros de la identidad y de la identificación en beneficio de la población y el efecto es alto.	La oportunidad tiene impacto directo en mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad y el efecto es alto.	La oportunidad tiene impacto directo en Intensificar los procesos para la identidad y la identificación digital de la población y el efecto es alto.	La oportunidad tiene impacto directo en fortalecer la gestión institucional y el efecto es alto.	La oportunidad tiene impacto directo en fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución y el efecto es alto.
MUY ALTO	5	La oportunidad tiene impacto directo, en los servicios de registros de la identidad y de la identificación en beneficio de la población y el efecto es muy alto.	La oportunidad tiene impacto directo en mejorar los servicios registrales de la identidad y de la identificación para la población en situación de vulnerabilidad y el efecto es muy alto.	La oportunidad tiene impacto directo en Intensificar los procesos para la identidad y la identificación digital de la población y el efecto es muy alto.	La oportunidad tiene impacto directo en fortalecer la gestión institucional y el efecto es muy alto.	La oportunidad tiene impacto directo en fortalecer el Sistema de Gestión del Riesgo de Desastres en la institución y el efecto es muy alto.

TABLA N° 05: MATRIZ DE PROBABILIDAD E IMPACTO O MAPA DE CALOR DE OPORTUNIDADES

PROBABILIDAD									
Prácticamente Seguro	5	BAJA	MODERADA	ALTA	MUY ALTA	MUY ALTA	5	Muy alto	IMPACTO
Probable	4	BAJA	MODERADA	MODERADA	ALTA	MUY ALTA	4	Alto	
Posible	3	BAJA	BAJA	MODERADA	MODERADA	ALTA	3	Moderado o medio	
Improbable	2	BAJA	BAJA	BAJA	MODERADA	MODERADA	2	Bajo	
Muy improbable	1	BAJA	BAJA	BAJA	BAJA	BAJA	1	Muy bajo	

TABLA N.° 06: RESPUESTA A LAS OPORTUNIDADES	
EXPLOTAR	Buscar eliminar la incertidumbre asociada con una oportunidad haciendo que la oportunidad definitivamente se concrete.
COMPARTIR	Compartir una oportunidad con terceros aumenta la capacidad que salga adelante.
MEJORAR	Modificar el "tamaño" de la oportunidad, aumentando positivamente la probabilidad y / o el impacto, buscando facilitar o fortalecer la causa de la oportunidad.
ACEPTAR	Aceptar que exista una oportunidad y explotar, compartir o mejorar cuando se presente las condiciones para implementarlas.

ANEXO N° 06
Reporte de Avance de la Gestión del Riesgo



Anexo N° 06 Reporte de Avance de la Gestion del Riesgo

Gerencia:

Fecha de Reporte:

Trimestre :

ITEM	PROCESO	AREA	CODIGO DEL RIESGO	RIESGO	NIVEL DE EXPOSICION	RESPUESTA	ACCIONES ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO	PLAZO PARA IMPLEMENTAR		NIVEL DE AVANCE				RESULTADO DEL INDICADOR	COMENTARIOS
								FECHA INICIO	FECHA FIN	% PROGRAMADO	% EJECUTADO	ESTADO			