RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA UNIVERSALIZACION DE LA SALUD"

Lima, 04 de Junio del 2020

RESOLUCION SECRETARIAL N° 000029-2020/SGEN/RENIEC

VISTOS:

El Informe N° 000015-2020/GG/OFCR/RENIEC (14FEB2020) y el Memorando Nº 000135-2020/GG/OFCR/RENIEC (10MAR2020) de la Oficina de Fiscalización, Control y Riesgos de la Gerencia General; el Memorando N° 000611-2020/GPP/RENIEC (20FEB2020) de la Gerencia de Planificación y Presupuesto; el Informe N° 000055-2020/GPP/SGRM/RENIEC (20FEB2020) de la Sub Gerencia de Racionalización y Modernización de la Gerencia de Planificación y Presupuesto; el Memorando Nº 000141-2020/GCI/RENIEC (13MAR2020) de la Gerencia de Calidad e Innovación; el Memorando N° 000197-2020/GG/RENIEC (28MAY2020) de la Gerencia General; el Informe N° 000718-2020/GAJ/SGAJA/RENIEC (05MAR2020) de la Sub Gerencia de Asesoría Jurídica Administrativa de la Gerencia de Asesoría Jurídica y la Hoja de Elevación N° 000148-2020/GAJ/RENIEC (05MAR2020) de la Gerencia de Asesoría Jurídica;

CONSIDERANDO:

Que el Registro Nacional de Identificación y Estado Civil es un organismo constitucionalmente autónomo, encargado de manera exclusiva y excluyente, de las funciones de organizar y actualizar el Registro Único de Identificación de las Personas Naturales, inscribir los hechos y actos relativos a su capacidad y estado civil, asimismo, de emitir los documentos que acreditan la identidad de las personas; para tal fin, desarrollará técnicas y procedimientos automatizados que permitan un manejo integrado y eficaz de la información;

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

Que las diversas áreas del RENIEC, en su constante compromiso de mejoramiento, vienen revisando su normativa a efectos de solicitar la aprobación de nuevos documentos normativos o en otros casos, se dejen sin efecto, con la finalidad de mejorar u optimizar las labores de cada una de ellas;

Que al respecto, la Oficina de Fiscalización, Control y Riesgos del RENIEC, como unidad orgánica de apoyo de la Gerencia General, en virtud de las funciones establecidas en el Reglamento de Organización y Funciones vigente, tiene entre sus funciones la de incorporar la gestión de riesgos en la institución y además, proponer la normativa específica de control interno, gestión de riesgos y fiscalización posterior;

Que en ese contexto, mediante los documentos de vistos, la Oficina de Fiscalización, Control y Riesgos de la Gerencia General, propone la aprobación del documento normativo Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, segunda versión, cuyo objetivo es establecer la metodología y estandarización para la implementación y sostenibilidad a la Gestión Integral del Riesgo, aplicada en la gestión institucional, para brindar una seguridad razonable en el logro de los objetivos estratégicos institucionales y el cumplimiento de las disposiciones legales y normativas del Estado;

Que a través del documento de vistos, la Gerencia de Planificación y Presupuesto, sobre la base de lo informado por la Sub Gerencia de Racionalización y Modernización, determina que el proyecto del documento normativo propuesto, se ajusta a los lineamientos dispuestos en la Directiva DI-200-GPP/001 “Lineamientos para la Formulación de los Documentos Normativos del RENIEC”, sexta versión, aprobada por Resolución Secretarial N° 55-2017/SGEN/RENIEC (28AGO2017);

Que mediante los documentos de vistos, la Gerencia de Asesoría Jurídica emite opinión señalando que, el documento normativo Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, segunda versión, presenta la consistencia legal pertinente y recomienda su aprobación; precisando que previamente deberá dejarse sin efecto el Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, primera versión, aprobado mediante Resolución Secretarial N° 000034-2019/SGEN/RENIEC (08ABR2019);

Estando a lo opinado por la Gerencia de Asesoría Jurídica y conforme a las facultades delegadas a la Secretaría General del Registro Nacional de Identificación y Estado Civil mediante la Resolución Jefatural N° 21-2019/JNAC/RENIEC (12FEB2019); el Reglamento de Organización y Funciones del RENIEC, aprobado por Resolución Jefatural N° 073-2016/JNAC/RENIEC (01ABR2016) y sus modificatorias;

SE RESUELVE:

Artículo Primero.- Dejar sin efecto el Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, primera versión, aprobado mediante Resolución Secretarial N° 000034-2019/SGEN/RENIEC (08ABR2019).

Artículo Segundo.- Aprobar el Manual MGIR-200-GG/OFCR/001 “Gestión Integral del Riesgo”, segunda versión, propuesto por la Oficina de Fiscalización, Control y Riesgos de la Gerencia General.

Artículo Tercero.- Encargar a la Gerencia de Planificación y Presupuesto la difusión del documento normativo aprobado.

Regístrese, comuníquese y cúmplase.

HRA/rae

MANUAL

GESTIÓN INTEGRAL DEL RIESGO

RESOLUCIÓN SECRETARIAL N° -2020/SGEN/RENIEC		
MGIR-200-GG/OFCR/001	VERSIÓN: 02	FECHA DE APROBACIÓN
	N° PÁGINAS: 71	

ÍNDICE

I. OBJETIVO

Establecer la metodología y estandarización para la implementación y sostenibilidad a la Gestión Integral del Riesgo, aplicada en la gestión institucional, para brindar una seguridad razonable en el logro de los objetivos estratégicos 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 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 sus modificatorias.

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

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

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

3.5 **Decreto Supremo Nº 015-98-PCM,** aprueba el Reglamento de Inscripciones del Registro Nacional de Identificación y Estado Civil, del 25 de abril de 1998 y sus modificatorias.

3.6 **Decreto Supremo Nº 030-2002-PCM**, aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado, del 03 de mayo de 2002.

3.7 **Decreto Supremo Nº 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. Nº 022-2002-MTC, el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por D.S. Nº 020-2007-MTC y el Reglamento de la Ley de Radio y Televisión, aprobado por D.S. Nº 005-2005-MTC; y deroga los DD.SS. Nº 030-2007-MTC y Nº 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 y sus modificatorias.

3.9 **Decreto Supremo Nº 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 02 noviembre de 2012 y sus modificatorias.

3.10 **Decreto Supremo N° 004-2013-PCM,** aprueba la Política Nacional de Modernización de la Gestión Pública, del 09 de enero de 2013.

3.11 **Decreto Supremo Nº 034-2014-PCM,** aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2014-2021, del 13 mayo de 2014.

3.12 **Decreto Supremo Nº 092-2017-PCM,** aprueba la Política Nacional de Integridad y Lucha contra la Corrupción, del 14 setiembre de 2017.

3.13 **Decreto Supremo Nº 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 Nº 050-2018-PCM,** aprueba la definición de 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 16 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 07 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 14 de enero de 2016 y sus modificatorias.

3.19 **Resolución Ministerial N° 119-2018-PCM,** dispone la creación de un Comité de Gobierno Digital en cada Entidad de la Administración Pública, del 10 de mayo de 2018, y su modificatoria.

3.20 **Resolución Ministerial N° 087-2019-PCM,** aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, del 22 de marzo de 2019.

3.21 **Resolución de Contraloría Nº 320-2006-CG**, aprueban Normas de Control Interno, del 03 de noviembre de 2006.

3.22 **Resolución de Contraloría Nº 146-2019-CG/INTEG**, aprueba la Directiva N° 006-2019-CG-INTEG "Implementación del Sistema de Control Interno en las entidades del Estado", del 17 de mayo de 2019

3.23 **Resolución Directoral N° 012-2017-INACAL/DN,** aprueban la Norma Técnica Peruana por los fundamentos de la presente resolución conforme al procedimiento establecido en la Ley N° 30224, NTP-ISO 37001:2017 Sistemas de Gestión Antisoborno. Requisitos con orientación para su uso. 1a Edición, del 04 de abril de 2017.

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

3.25 **Resolución Jefatural Nº 073-2016-JNAC-RENIEC**, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 01 de junio de 2016 y modificatorias.

3.26 **Resolución Jefatural N° 020-2019/JNAC/RENIEC,** designa Oficial de cumplimiento del Sistema de Gestión Antisoborno del Registro Nacional de Identificación y Estado Civil, del 08 de febrero 2019.

3.27 **Resolución Jefatural N° 021-2019/JNAC/RENIEC**, delega a la Secretaría General la facultad, entre otras, de aprobar documentos normativos, del 11 de febrero de 2019.

3.28 **Resolución Jefatural N° 70-2019/JNAC/RENIEC,** aprueba el Plan Estratégico Institucional 2018-2022 del RENIEC, del 03 mayo de 2019.

3.29 **Resolución Jefatural N° 03-2020/JNAC/RENIEC**, reconforman el Comité de Gobierno Digital del Registro Nacional de Identificación y Estado Civil, del 07 de enero de 2020.

3.30 **Resolución Jefatural N° 137-2019/JNAC/RENIEC**, aprueba los productos priorizados propuestos y consensuados, en cumplimiento de la norma establecida en el inciso a) del subnumeral 6.5.1 de la Directiva DI-006-2019-CG/INTEG "Implementación del

Sistema de Control Interno en las Entidades del Estado" aprobada por la Resolución Contraloría N° 146-2019-CG (15MAY2019), del 12 de setiembre de 2019.

3.31 **Resolución Jefatural N° 162-2019/JNAC/RENIEC**, designa a la Secretaría General del RENIEC como el Órgano responsable de la implementación del Sistema de Control Interno (SCI) y dispone que la Oficina de Fiscalización, Control y Riesgos, coordine con la Secretaría General la ejecución de las acciones necesarias para la implementación del SCI, del 30 de setiembre de 2019.

3.32 **Resolución Jefatural N° 186-2019/JNAC/RENIEC,** aprueba la actualización de la Política de la Gestión Integral del Riesgo y Objetivos de la Gestión Integral del Riesgo en el RENIEC, del 11 de noviembre de 2019 y rectificatoria**.**

3.33 **Resolución Secretarial Nº 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.

3.34 **Resolución Secretarial Nº 107-2019/SGEN/RENIEC,** aprueba la Directiva DI-438-GCI/017 "Implementación de la Gestión por Procesos en el RENIEC", del 09 de octubre del 2019.

3.35 **Resolución Secretarial Nº 112-2019/SGEN/RENIEC,** aprueba el Mapa de Procesos de nivel 0 y 1 de los procesos transversales del RENIEC, del 18 de octubre de 2019.

3.36 **Resolución Secretarial Nº 000027-2020/SGEN/RENIEC,** aprueba la Directiva DI-418-GG/OFCR/002 "Gestión Integral del Riesgo", del 25 de mayo de 2020.

IV. DEFINICIÓN DE TÉRMINOS

4.1 **Amenaza**

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

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

Para riesgos de desastres es la potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas.

4.2 **Confidencialidad**

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

4.3 **Contexto Externo**

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

4.4 **Contexto Interno**

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

4.5 **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.

4.6 **Control existente/implementado**

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

4.7 **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.

4.8 **Criterios del Riesgo**

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

4.9 **Dueño del Riesgo**

Dueño del proceso o Gerente designado que gestiona el proceso; con responsabilidad y autoridad para gestionar el riesgo.

4.10 **Disponibilidad**

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

4.11 **Equipo de Riesgos**

Grupo multifuncional conformado por el Gestor Líder de Riesgos y personal de los Órganos con conocimientos en riesgos y procesos que gestiona los riesgos y reporta sus resultados. Es designado por el Dueño del Riesgo.

4.12 **Equipo técnico de Gestión Integral del Riesgo**

Grupo de especialistas encargados de brindar apoyo técnico a la Alta Dirección y Órganos de la Entidad en el proceso de la Gestión Integral del Riesgo. Está conformado por la OFCR, OSDN, GCI, Oficial de Seguridad de la Información y Oficial del Sistema de Gestión Antisoborno.

4.13 **Evento de pérdida**

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

4.14 **Fuente de Riesgo**

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

4.15 **Gestión Integral del Riesgo**

Es la aplicación sistemática de políticas, procedimientos y prácticas de gestión que brindan una seguridad razonable para el cumplimiento de los objetivos institucionales. Se implanta como un sistema de gestión que constituye una herramienta para la toma de decisiones y que permite integrar otros sistemas de gestión reconocidos, como el de gestión de la calidad ISO 9001, gestión ambiental ISO 14001, gestión de seguridad y salud en el trabajo ISO 45001, seguridad de la información ISO 27001, sistema de gestión antisoborno ISO 37001, o cualquier otro sistema de gestión basado en el ciclo de mejora continua.

4.16 **Gestor Líder de Riesgos**

Responsable designado por el Órgano correspondiente, quien realizará las coordinaciones con los Órganos de asesoramiento técnico encargados de la Gestión Integral del Riesgo.

4.17 **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.

4.18 **Impacto o Consecuencias**

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

4.19 **Incidente de Seguridad de Información**

Uno o una serie de eventos de pérdida de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones y amenazan la Seguridad de la Información del RENIEC.

4.20 **Integridad**

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

4.21 **Medida de Control**

Es la acción que permite tratar el riesgo, reduciendo la probabilidad de ocurrencia, y/o el impacto potencial del riesgo identificado.

4.22 **Plan de Acción Anual – Medidas de Control (PAAMC) o Plan de Gestión Integral del Riesgo**

Documento donde se registran las acciones para gestionar los riesgos identificados que requieren tratamiento.

4.23 **Plan de Contingencia**

Documento que contiene las acciones de ejecución inmediata en respuesta al riesgo materializado. Forma parte del Plan de Acción Anual – Medidas de Control (PAAMC) o Plan de Gestión Integral del Riesgo.

4.24 **Política de la Gestión Integral del Riesgo**

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

4.25 **Probabilidad**

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

4.26 **Producto**

Bien o servicio que proporciona la Entidad a una población beneficiaria con el objeto de satisfacer sus necesidades.

4.27 **Producto Priorizado**

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

4.28 **Proceso Gestión Integral del Riesgo**

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

4.29 **Riesgo**

Es la posibilidad de ocurrencia de un evento adverso o positivo, respecto al cumplimiento de los objetivos estratégicos institucionales.
Efecto de la incertidumbre sobre la consecución de los objetivos. (ISO NTP 31000:2018).

4.30 **Riesgo Aceptado**

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

4.31 **Riesgo Residual**

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

4.32 **Seguimiento, Medición y Control**

Proceso de evaluación permanente de la Gestión del Riesgo en la Entidad a cargo de la OFCR en coordinación con el equipo técnico de la Gestión Integral del Riesgo.

4.33 **Seguimiento y Revisión**

Proceso de seguimiento permanente y evaluación periódica durante la ejecución del proceso de la Gestión Integral del Riesgo a cargo de los Dueños del Riesgo.

4.34 **Servicio Digital**

Es aquel que se provee 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.

4.35 **Vulnerabilidad**

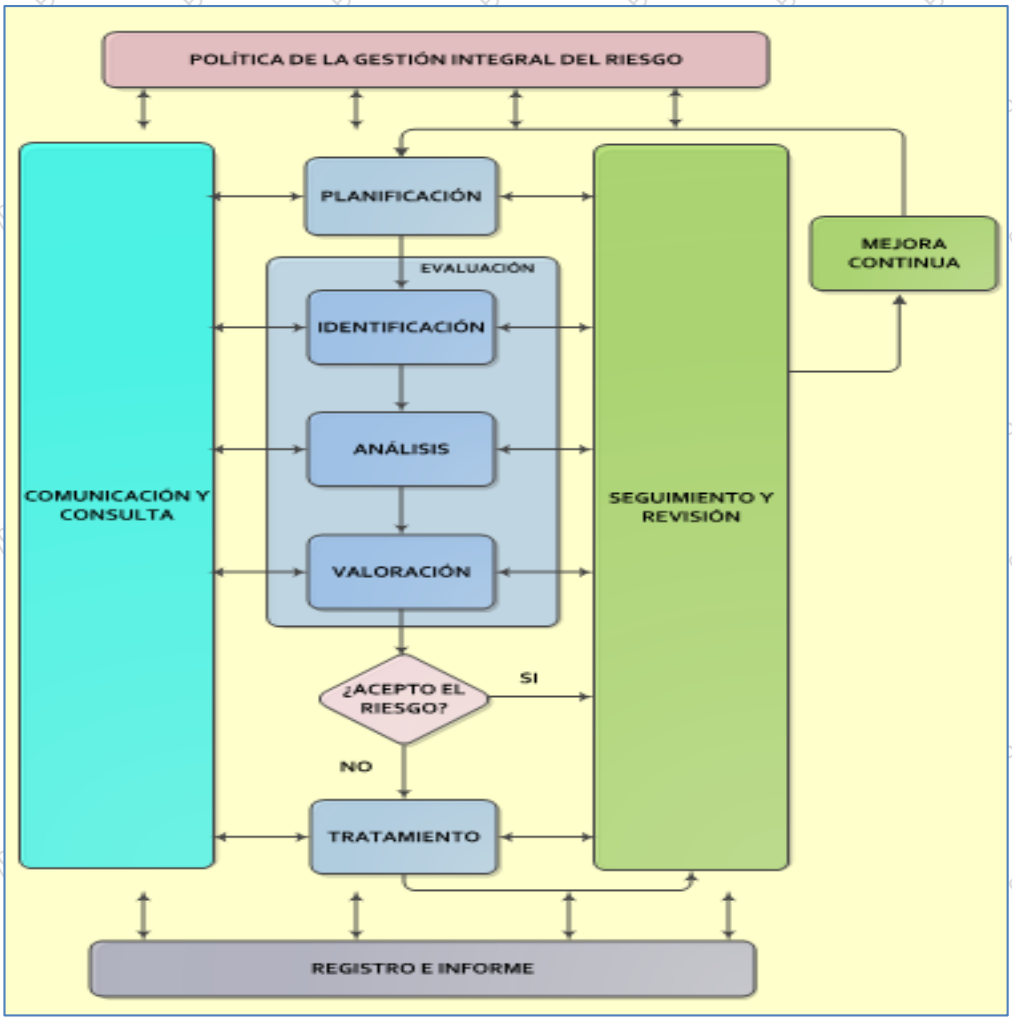
Debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes. Ausencia o debilidad de un control que puede ser explotado por una o más amenazas.

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 alentados 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 el tratamiento de todos los tipos de riesgos que se podrían identificar en la Entidad. La presente metodología debe ser aplicada por todos los Órganos de la Entidad. El Proceso de Gestión Integral del Riesgo se describe en el siguiente gráfico:

Gráfico N° 1: Proceso Gestión Integral del Riesgo



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

Los Órganos que tienen la competencia funcional en los Sistemas de Gestión (Gerencia de Calidad e Innovación, Oficina de Seguridad y Defensa Nacional), y Oficial de Cumplimiento Sistema de Gestión Antisoborno; pueden formular documentos normativos y formatos complementarios que sean necesarios para su gestión, para aquellos que cuentan con Sistemas de Gestión certificados.

EL PROCESO DE GESTIÓN INTEGRAL DEL RIESGO COMPRENDE LAS SIGUIENTES ACTIVIDADES:

5.1 PLANIFICACIÓN

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

5.1.1 ALCANCE DE LA GESTION INTEGRAL DEL RIESGO

El RENIEC ha definido su alcance en la Gestión Integral del Riesgo, considerando su aplicación en los niveles estratégico, táctico y operacional; principalmente, en sus productos (priorizado y no priorizado), procesos, proyectos, los Sistemas de Gestión con Certificación ISO para la toma de decisiones, la seguridad de la infraestructura y de las personas, la continuidad operativa; alineado a los objetivos estratégicos de la Entidad.

Este alcance es coherente con el desarrollo y ejecución de la Política de Gestión Integral del Riesgo alineada con sus objetivos estratégicos institucionales. Su implantación (en los niveles estratégico, táctico y operativo) se realiza como componente del Sistema de Control Interno y teniendo como base la gestión por 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 el Titular de la Entidad, la Alta Dirección y los Órganos de la Entidad, como parte esencial de la asignación de responsabilidades en las actividades para la Gestión Integral del Riesgo y la generación del pensamiento basado en riesgos como parte de la cultura de la Entidad. El compromiso por parte de los funcionarios y servidores civiles, ayuda a que la gestión de riesgos se integre en todos los niveles de la Entidad.

5.1.2 MARCO DE REFERENCIA

5.1.2.1 <u>Generalidades</u>

Lograr que la Gestión Integral del Riesgo se incorpore en todas las actividades y funciones significativas de la Entidad, su eficacia dependerá de su integración en la gobernanza de la Entidad. Por lo tanto, se requiere el apoyo de la Alta Dirección y de las partes interesadas.

5.1.2.2 <u>Liderazgo y Compromiso</u>

El Jefe Nacional, Secretario General y Gerente General, aseguran que la Gestión Integral del Riesgo se incorpore progresivamente en todas las actividades de la organización, contribuyendo a que la Entidad implemente una cultura basada en riesgos y pueda alinearla con sus objetivos estratégicos institucionales.

Gráfico N° 2: Marco de Referencia de la GIR

Fuente: NTP-ISO 31000:2018.

5.1.2.3 **Integración**

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

Gráfico N° 3: Articulación de los Sistemas de Gestión

Fuente: Elaboración OFCR

5.1.2.4 **Diseño**

5.1.2.4.1 **Comprensión de la Entidad y su contexto**

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

Con la finalidad de identificar riesgos que puedan afectar los objetivos del proceso evaluado, el Gestor Líder de Riesgos y el equipo de Riesgos deben realizar previamente el análisis del contexto externo e interno, así como las partes interesadas, mediante el formato aprobado por el Órgano técnico responsable de la Entidad.

A. **El contexto interno**

Para establecer el contexto interno, se debe considerar los siguientes aspectos:

a) 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.

b) El modelo de gestión de riesgos incorporado a la planificación estratégica (misión, visión, valores, liderazgo, estructura organizacional y cultura organizacional).

c) Los procesos, planes, proyectos, activos, sistemas de gestión y procedimientos para la toma de decisiones

d) Los 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.

e) La administración de los recursos (capacidades y competencias del personal, condiciones de trabajo, sistemas de información y tecnologías, flujos de información), la Alta Dirección y los Órganos competentes deberán asegurar la asignación los recursos apropiados para la Gestión Integral del Riesgo.

f) Los 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.

g) Las principales fuentes de consulta a utilizar: PEI, POI, ROF, MOF, CAP, PAP, PDP, Mapa de Procesos, otros informes, planes, programas, proyectos de importancia institucional que permitan conocer o determinar los objetivos y resultados sobre los que impacta el riesgo.

B. **El contexto externo**

Para establecer el contexto externo, se debe considerar los distintos ámbitos, tales como: Internacional, nacional, regional y local; y atribuye aspectos culturales, sociales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos, medioambientales, entre otros.

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

La Alta Dirección y los Órganos del RENIEC deberán articular y demostrar su compromiso, expresándose claramente mediante una política, una declaración u otras formas.

5.1.2.4.3 **Establecimiento de la comunicación y consulta**

La comunicación implica compartir información con las partes interesadas. El RENIEC cuenta con mecanismos de comunicación y consulta pertinentes, tales como: Sistema Integrado de Tramite Documentario, correo electrónico institucional, intranet, micro sitio, entre otros.

5.1.2.5 **Implementación**

El RENIEC implementa la Gestión Integral del Riesgo mediante el desarrollo del Plan de Acción Anual – Medidas de Control (PAAMC).

5.1.2.6 **Valoración**

Para medir la eficacia de la Gestión Integral del Riesgo, el RENIEC evalúa periódicamente su desempeño con relación a sus metas, planes e indicadores.

5.1.2.7 **Mejora**

Realizar el seguimiento continuo de la Gestión Integral del Riesgo en función a los cambios externos e internos.

5.1.3 GESTIÓN DE EVENTOS DE PÉRDIDA

Con la finalidad de contar con un registro que permita detectar, analizar, responder y reportar los eventos de pérdida o incidentes identificados en los procesos asociados a riesgos que puedan afectar el cumplimiento de los Objetivos Estratégicos Institucionales, se ha elaborado un formato que permitirá contar con un registro interno de incidentes y eventos de pérdida.

Para la gestión de los incidentes de Seguridad de la Información, se debe utilizar los lineamientos establecidos en los documentos normativos de la Sub Gerencia de Seguridad de la Información de la Oficina de Seguridad y Defensa Nacional (OSDN/SGSI).

Actividades para el registro y reporte de incidentes o eventos de pérdida

Los Órganos deben reportar los eventos de pérdida cuando el evento se haya materializado; dicho reporte se realizará mediante el Registro N° 1, Reporte de Eventos de Pérdida contenidas en el Anexo N° 01.

Las actividades que debe realizar el Gestor Líder de Riesgos conjuntamente con el Equipo de Riesgos para comunicar los incidentes o eventos de pérdida en sus procesos, serán las siguientes:

Nro. de Actividad	Descripción de la actividad
1	Anotar en el Registro N° 1: Eventos de Pérdida, que se encuentran en el Anexo N° 01.
2	Para el registro en los campos descripción, tipo evento de pérdida, categoría de evento de pérdida, efectos de evento de pérdida y respuesta de evento de pérdida, que se encuentran en el Registro N° 1, se deberá tomar en cuenta la Tabla N° 1: Tipos de Eventos de Pérdida por Riesgos, que se encuentran en el Anexo N° 01.
3	Describir el incidente y/o evento de pérdida, las causas, los efectos y la respuesta.
4	Registrar la fecha de implementación, acciones de seguimiento y revisión realizadas y el estado.

5.1.4 CRITERIOS PARA LA GESTIÓN INTEGRAL DEL RIESGO

El RENIEC, de acuerdo a su estructura determina la cantidad y tipos de riesgo relacionados a sus productos, procesos y actividades; dentro de los cuales se encuentran: corrupción, cumplimiento, desastres, estratégico, financiero, imagen, operativo, proyectos, seguridad de la información, seguridad y salud en el trabajo, tecnológico, entre otros.

La Entidad ha definido los niveles de probabilidad (baja, media, alta y muy alta) e impacto (bajo, medio, alto y muy alto). Así como los niveles de exposición al riesgo (bajo, medio, alto y muy alto). Asimismo, para el nivel de exposición **bajo,** ha establecido acciones de seguimiento y revisión permanente por parte del Dueño del Riesgo, con la finalidad que se mantengan en el nivel aceptado.

Sobre aquellos riesgos con niveles de exposición **medio, alto y muy alto** se debe establecer un plan de tratamiento (medidas de control). Para el caso de las oportunidades con nivel de exposición **alto y muy alto**, corresponde definir las acciones para perseguir las mismas.

Los riesgos identificados son registrados en el **Plan de Acción Anual - Medidas de Control (PAAMC) o Plan de Gestión Integral del Riesgo**, cuyo documento es aprobado por el titular de la Entidad, el cual contiene el tratamiento (medidas de control) de los mismos en los productos priorizados con niveles de exposición **medio, alto y muy alto.** El PAAMC es reportado a la Contraloría General de la República (CGR). En los casos de los riesgos identificados en los procesos cuyos productos no formen parte de los productos priorizados, los Órganos deben gestionar su tratamiento.

Para la Gestión Integral del Riesgo los Órganos cuentan con el marco normativo para su aplicación, así como el soporte de los Órganos competentes quienes brindarán la asistencia técnica.

Los riesgos de Seguridad y Salud en el Trabajo, se gestionan de acuerdo a las normas internas específicas vigentes.

El RENIEC en cumplimiento de la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del estado", aprobada por la CGR, ha incorporado la gestión de los riesgos de corrupción la cual será implementada progresivamente en la Entidad, con la finalidad de aplicar controles que permitan prevenir, detectar y responder eficazmente a los riesgos de corrupción.

5.1.5 REGISTRO DEL PROCESO Y PRODUCTO

El Líder de Riesgos y el Equipo de Riesgos deben identificar el proceso y producto que se debe registrar en el **PAAMC**. Es necesario que se identifiquen los riesgos en todos los procesos que participan en la provisión del producto.

La información se registrará en el Registro N° 2: Plan de Acción Anual -Medidas de Control o Plan de Gestión Integral del Riesgo) del Anexo N° 02, el cual contiene todas las etapas del proceso de Gestión Integral del Riesgo.
El riesgo será identificado a nivel del **"Diagrama flujo Actividades"** del proceso evaluado.

Gráfico N° 4: Identificación del Proceso

.

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 (GOR).

Ejemplo:

IDENTIFICACIÓN DEL PROCESO Y PRODUCTO					
PROCESO NIVEL 1	CODIGO DEL PROCESO DEL NIVEL DESAGREGADO (*)	PROCESO NIVEL DESAGREGADO (*)	OBJETIVO DEL PROCESO	ORGANO RESPONSABLE DEL PROCESO	PRODUCTO PRIORIZADO
Proceso de Identificación	PM01.01.03	Entrega de DNI	Entregar el DNI a los ciudadanos cumpliendo los procedimientos establecidos.	**GOR**	**Población cuenta con DNI**

(*) Corresponde al proceso a nivel de diagrama de flujo definidos por el Órgano técnico 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) con la Entidad, para el logro de sus objetivos, por ello es importante contar con información apropiada y actualizada.

En la identificación de los riesgos del proceso se debe considerar el análisis del contexto externo e interno y las partes interesadas, teniendo presente los objetivos para precisar el alcance del proceso, proyecto, producto (priorizado y no priorizado), servicio, activo, sistema de gestión u otros.

Debiendo seleccionarse uno de los métodos de la Tabla N° 2: Técnicas utilizadas en la Gestión del Riesgo del Anexo N° 02, 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. Asimismo, se debe utilizar la Tabla N° 3: Preguntas Guía para la Identificación de Riesgos del Anexo N° 02.

- Para el análisis de los efectos (consecuencias) del riesgo identificado en el proceso, producto (priorizado y no priorizado), actividades y tareas, se debe considerar la locación; el comportamiento y capacidades humanas, la organización del trabajo y otros factores humanos; servicios de apoyo y equipamiento, gestión de proveedores, subcontratación de actividades; infraestructura, tipos de producto y/o servicios; cambios o propuestas, utilizando el Registro Nº 2: Plan de Acción Anual – Medidas de Control o Plan de Gestión Integral del Riesgo, del Anexo N° 02.

- Cuando se identifiquen riesgos en el proceso en los que participan otros Órganos, el Dueño del riesgo debe coordinar con éstos, para determinar las causas y consecuencias de la materialización del Riesgo y de considerarlo necesario coordinar la participación del Equipo Técnico de Gestion Integral del Riesgo.

<u>Identificación de los Riesgos de Corrupción</u>

Para la identificación de riesgos de corrupción se debe considerar: Tabla N° 20: Situaciones susceptibles de Riesgos de Corrupción, Tabla N° 21: Preguntas Guía para identificar Riesgos de Corrupción del Anexo Nº 03, en la que se listan preguntas que sirven de orientación.

Es importante precisar que el riesgo debe estar descrito de manera clara y precisa, su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Con el fin de facilitar la redacción del riesgo de corrupción y evitar que se presenten confusiones entre el riesgo de corrupción y los otros tipos de riesgos, se debe utilizar la Tabla N° 22: Criterios para identificar el Riesgo de Corrupción del Anexo N° 03, que incorpora cada uno de los componentes de su definición.

- El riesgo de corrupción identificado debe ser evidenciado en el Registro Nº 2: Plan de Acción Anual – Medidas de Control (PAAMC) o Plan de Gestión Integral del Riesgo, del Anexo N° 02.

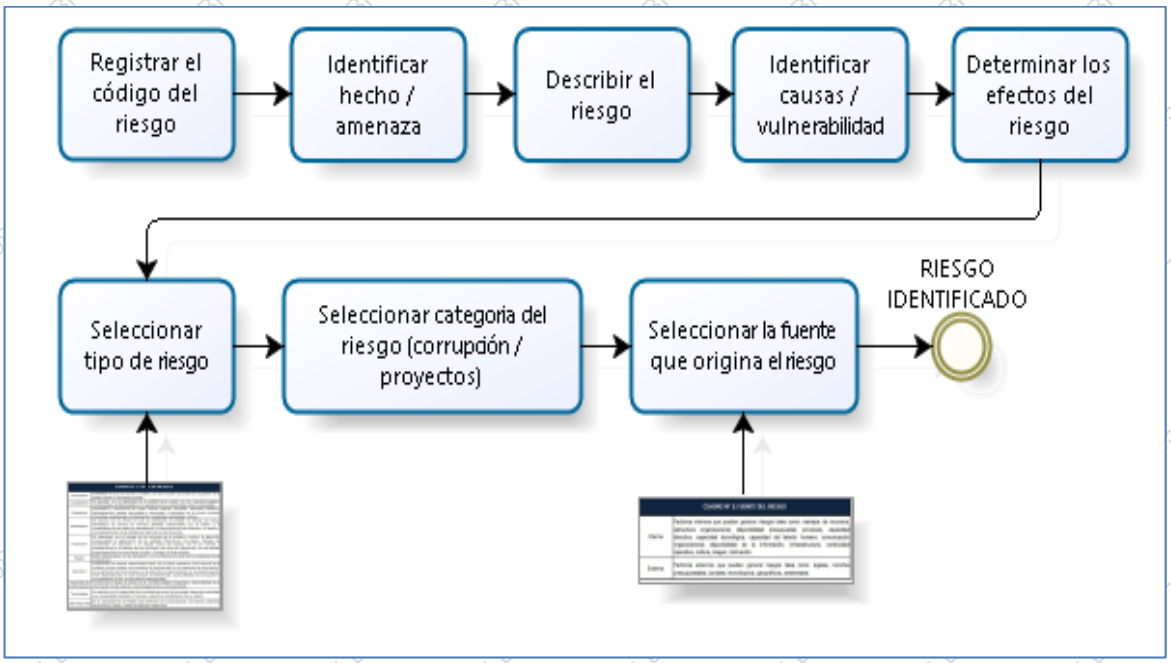
Actividades para la identificación del Riesgo en el proceso

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

N° de Actividad	Descripción de la actividad
1	Registrar el código del riesgo de acuerdo a la siguiente estructura: CODIGO DEL PROCESO + "_" + R + Número Correlativo **EJEMPLO: PM01.01_R01** **DONDE:** **CODIGO DEL PROCESO:** Es el código asignado a cada proceso definido por el Órgano Técnico 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	Registrar la **descripción de riesgos** de acuerdo a la siguiente estructura: Debido a la <**CAUSA/VULNERABILIDAD**> puede ocurrir el **<HECHO/ AMENAZA/RIESGO>**, lo que provocaría el **<EFECTO o CONSECUENCIA>** Registrar la descripción de **riesgos de corrupción** de acuerdo a la siguiente estructura: **Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**
4	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.
5	Registrar los efectos o consecuencias del riesgo materializado.

6	Seleccionar el tipo de riesgo de acuerdo a la Tabla N° 4 Tipos de Riesgo - Anexo N° 02
7	Para riesgos de Corrupción: Seleccionar la categoría de acuerdo a la Tabla N° 22 Tipos de Corrupción - Anexo N° 03 Para riesgos de Proyecto: Seleccionar la categoría de acuerdo a la Tabla N° 5 Categoría de Riesgo de Proyecto - Anexo N° 02
8	Seleccionar la fuente del riesgo según su origen (interno o externo). Tabla N° 6 Fuente del Riesgo - Anexo N° 02

Gráfico N° 5: 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 y Desastres)	DESCRIPCIÓN DEL RIESGO	CAUSAS O VULNERABILIDAD	EFECTOS	TIPO DE RIESGO (TABLA N° 4)	CATEGORIA DEL RIESGO (CORRUPCION/ PROYECTOS) (TABLA N° 5, 23)	FUENTE QUE ORIGINA EL RIESGO (TABLA N° 6)
P01.01.01.03_R01		Debido a las deficiencias en la verificación de la identidad durante la entrega del DNI de mayor de edad en los locales de atención, podria ocasionar que el documento nacional de identidad sea entregado a persona distinta del titular generando perjuicio al ciudadano por uso indebido.	♦ 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 biometricos 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.	OPERATIVO		INTERNA

DESASTRES
ESTRATÉGICO
FINANCIERO
IMAGEN
OPERATIVO
PROYECTOS
SEGURIDAD DE LA
TECNOLÓGICO

INTERNA
EXTERNA

Para el caso de la identificación de los riesgos de Seguridad de la Información será necesario previamente realizar un inventario de activos de información, de acuerdo a los lineamientos que establezca la OSDN/SGSI.

5.3 ANÁLISIS Y VALORACIÓN DEL RIESGO

5.3.1 ANÁLISIS DEL RIESGO

Consiste en determinar la probabilidad y el impacto (consecuencias). El análisis del riesgo debe considerar factores como:

A. **La probabilidad** de ocurrencia de los eventos, en términos de frecuencia (eventos ocurridos en un determinado periodo de tiempo, revisar el registro de incidentes o eventos de pérdida) o factibilidad (presencia de factores externos – internos que pueden propiciar el riesgo), para la evaluación de la probabilidad se debe utilizar la Tabla N°7 Niveles de Probabilidad del Anexo N° 02.

B. **El impacto** (consecuencias) que afecta a los objetivos pueden ser negativo o positivo, para la evaluación del impacto se debe utilizar la Tabla N° 8 Niveles de Impacto para riesgos en general, Tabla N° 9 Niveles de Impacto para riesgos en Seguridad de la Información y la Tabla N° 10 Niveles de Impacto para riesgo en Proyectos del Anexo N° 02, según corresponda al tipo de riesgo identificado. En el presente manual se han definido los siguientes criterios de impacto:

a) **Objetivos Estratégicos Institucionales (OEI)**; el grado en que el riesgo afecta los resultados y el cumplimiento de los objetivos estratégicos institucionales. Como referencia se tendrá en cuenta el cumplimiento del Plan Estratégico Institucional (PEI) y Plan Operativo Institucional (POI).

b) **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.

c) **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.

d) **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.

e) **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.

- La probabilidad y el impacto se combinan para determinar el nivel de exposición al riesgo. Tabla N° 11 Mapa de Riesgos del Anexo N° 02.

Análisis de los Riesgos de Corrupción

a) Para la evaluación de la probabilidad de ocurrencia en los riesgos de corrupción se debe utilizar la Tabla N° 7 Niveles de Probabilidad - Anexo N° 02.

b) Para la evaluación del impacto en los riesgos de corrupción se debe utilizar el Registro N° 04 Criterios para evaluar el Impacto en Riesgos de Corrupción del Anexo N° 03.

c) Para determinar el nivel de exposición de riesgos de corrupción se debe realizar el análisis teniendo en cuenta **solo** los niveles de impacto **"alto" y "muy alto"**, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto **bajo y medio**, que sí aplican para los demás riesgos. Ver Tabla N° 23 Mapa de Riesgos de Corrupción del Anexo N° 03.

Análisis y Evaluación de Controles Existentes

En esta etapa se debe realizar la evaluación del control y/o controles existentes para todos los tipos de riesgos en el Registro N° 3 Evaluación de Controles existentes/implementados del Anexo N° 02, para lo cual se deben utilizar las Tablas N° 12 Tipos de Control existente/implementado, N° 13 Criterios para el análisis del control existente/implementado y la N° 14 Rangos del resultado de la calificación del control existente/implementado - Anexo N° 02.

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

5.3.2 VALORACIÓN DEL RIESGO

Implica comparar los resultados del análisis del riesgo con el criterio de aceptación, donde se debe establecer medidas de control para tratar los riesgos que presenten niveles de exposición **medio, alto y muy alto.** Esta comparación determina la decisión sobre la necesidad, prioridad, recursos y características del tratamiento, así como la determinación de las Medidas de Control para gestionar el riesgo.

Actividades para el Análisis y Valoración del Riesgo en el proceso

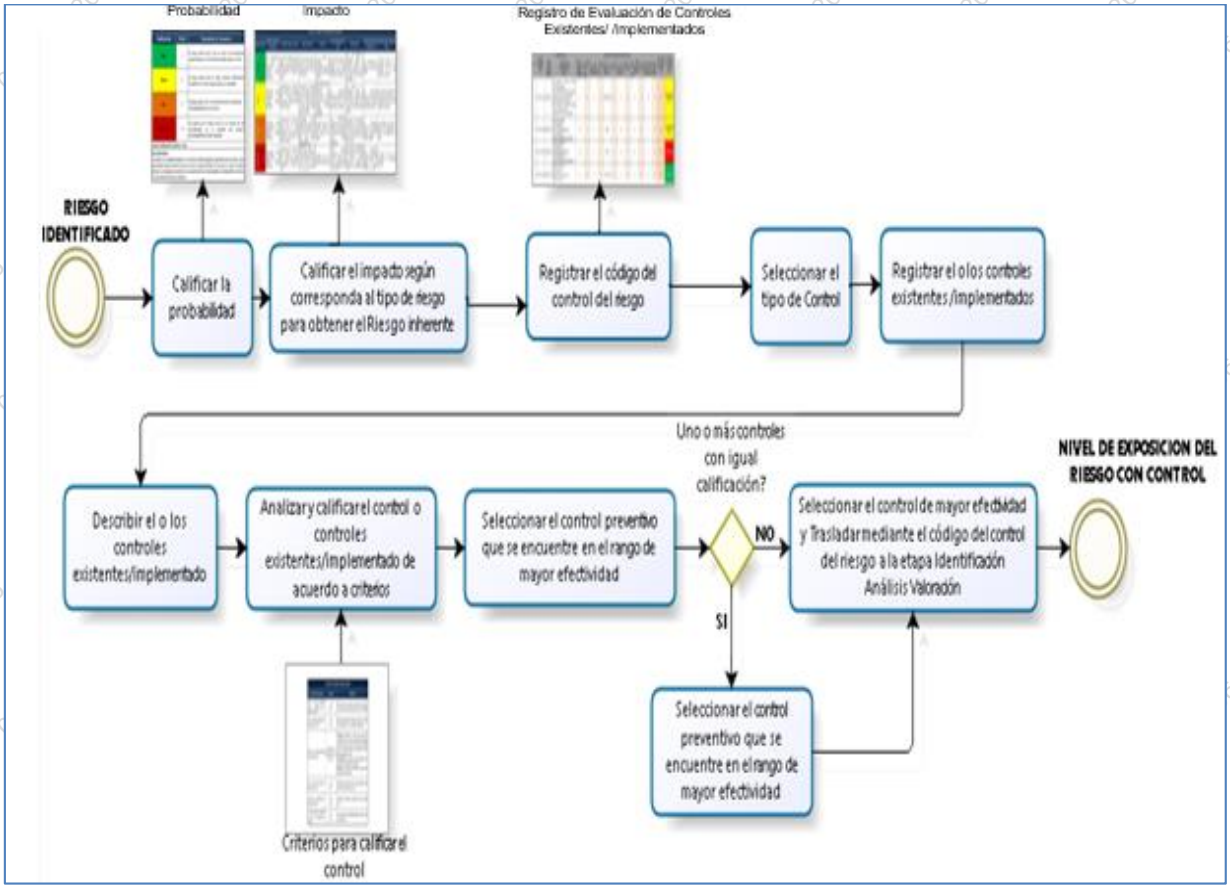
Las actividades que debe realizar el Gestor Líder de Riesgos y el Equipo de Riesgos en la etapa de análisis y valoración del riesgo en su proceso, serán las siguientes:

Nº de Actividad	Descripción de la actividad
9	Seleccionar y calificar la probabilidad de ocurrencia utilizando la Tabla N° 7 Niveles de Probabilidad - Anexo N° 02.
10	Calificar el impacto de acuerdo a los criterios establecidos en las Tablas Nº 8, 9, 10 - Anexo N° 2, según corresponda por el tipo de riesgo. Para calificar el impacto en los riesgos de corrupción se debe utilizar el Registro N° 4 Criterios para evaluar el Impacto en Riesgos de Corrupción del Anexo N° 03. Como resultado de la calificación de la probabilidad por el impacto, obtenemos el riesgo inherente el cual conjuntamente con la evaluación de controles existentes/implementados nos da como resultado el nivel de exposición del riesgo con control.
11	Registrar el o los controles existentes según corresponda, para lo cual se debe utilizar el Registro N° 3 Evaluación de Controles existentes/implementados del Anexo N° 02.
12	En el Registro N° 3 Evaluación de Controles existentes/implementados del Anexo Nº 02 se debe realizar lo siguiente: 12.1 Registrar el código del control del riesgo de acuerdo a la siguiente estructura: CODIGO DEL PROCESO + "_" + C + Número Correlativo 12.2 Seleccionar el tipo de control, para lo cual debe utilizar la Tabla N° 12 Tipos de Control existente/implementado del Anexo Nº 02. 12.3 Registrar el código del control existente. 12.4 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? 12.5 Calificar el control o controles existentes de acuerdo a la Tabla N° 13 Criterios para el análisis del control existente/implementado del Anexo Nº 02. 12.6 Seleccionar el control con mayor nivel de efectividad de acuerdo a la Tabla N° 14 Rangos del resultado de la calificación del control existente/implementado del Anexo N° 02 (*). 12.7 Trasladar los datos del control seleccionado al Registro Nº 2: Plan de Acción Anual – Medidas de Control o Plan de Gestión Integral del Riesgo del Anexo Nº 02, 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.

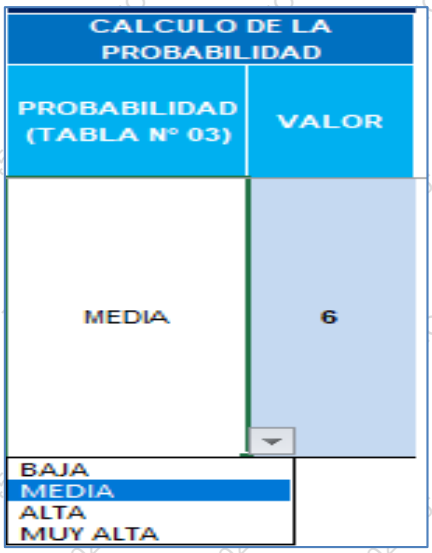
Como resultado de estas actividades se debe obtener el nivel de exposición del riesgo con control que nos servirá para tomar una decisión para el tratamiento del riesgo.

Gráfico N° 6: 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.



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

CRITERIOS DE IMPACTO (TABLA N° 8)					
OBJETIVOS ESTRATEGICOS INSTITUCIONALES	CUMPLIMIENTO LEGAL Y NORMATIVO	IMAGEN INSTITUCIONAL	OPERATIVIDAD	IMPACTO (TABLAS N° 8, 9, 10, Registro 5)	VALOR
MEDIO	BAJO	MEDIO	BAJO	MEDIO	6

BAJO
MEDIO
ALTO
MUY ALTO

Como resultado de la calificación de la probabilidad por el impacto obtenemos el riesgo inherente. A continuación, en el Registro N° 3 Evaluación de Controles existentes/implementados del Anexo N° 02, se debe registrar 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 / IMPLEMENTADO	
	TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE / IMPLEMENTADO
P08.01.03.03_C001	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.

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

CRITERIOS PARA LA EVALUACIÓN DEL CONTROL EXISTENTE/IMPLEMENTADO												CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA N° 13)
¿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?			
NO	0	SI	10	SEMIAUTOMATICO	10	SI	10	SI	25	NO	0	55	NO EFECTIVO

Trasladar los datos del control seleccionado al Registro Nº 2: Plan de Acción Anual – Medidas de Control o Plan de Gestión Integral del Riesgo del Anexo Nº 02, registrando el

código del control del riesgo de acuerdo al siguiente cuadro.

EVALUACION DEL CONTROL EXISTENTE / IMPLEMENTADO			CALIFICACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL ACTUAL (TABLA N° 14)
CODIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA N° 13)		
P08.01.03.03_C001	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.	55	NO 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 DEL RIESGO CON CONTROL						
PROBABILIDAD (TABLA N° 7)	VALOR	IMPACTO (TABLAS N° 8, 9, 10, Registro 6)	VALOR	P X I	NIVEL DE EXPOSICIÓN DEL RIESGO (TABLA N° 11)	ACCION A REALIZAR
ALTA	8	MEDIO	6	48	RIESGO ALTO	EL RIESGO DEBE SER TRATADO

Para el ejemplo podemos visualizar que **no** se ha reducido el nivel de exposición del riesgo por efecto del control existente; al tener un control calificado como control no efectivo, el riesgo mantiene su nivel de exposición como **Riesgo Alto**.

			IMPACTO			
			BAJO	MEDIO	ALTO	MUY ALTO
			4	6	8	10
PROBABILIDAD	MUY ALTA	10	40 RIESGO MEDIO	60 RIESGO ALTO	80 RIESGO MUY ALTO	100 RIESGO MUY ALTO
	ALTA	8	32 RIESGO MEDIO	48 RIESGO ALTO	64 RIESGO ALTO	80 RIESGO MUY ALTO
	MEDIA	6	24 RIESGO BAJO	36 RIESGO MEDIO	48 RIESGO ALTO	60 RIESGO ALTO
	BAJA	4	16 RIESGO BAJO	24 RIESGO BAJO	32 RIESGO MEDIO	40 RIESGO MEDIO

5.4 TRATAMIENTO DEL RIESGO

Tiene como objetivo diseñar, evaluar, seleccionar e implementar medidas de control para modificar el nivel de exposición de los riesgos. La implementación del tratamiento proporciona nuevos controles o modifica los existentes.

Para determinar la respuesta al riesgo se debe tener en cuenta los criterios establecidos por la Entidad y priorizar aquellos con un mayor nivel de exposición al riesgo, considerando la evaluación costo – beneficio. Una vez identificado el nivel de exposición al riesgo con control, se debe utilizar la Tabla N° 15 Tipos de Respuesta al Riesgo - Anexo N° 02, para determinar la respuesta al riesgo: Evitar, Reducir, Compartir o Aceptar.

Los riesgos de nivel **bajo** son aceptados por la Entidad, estos deben ser monitoreados constantemente con la finalidad que no varíen su nivel de exposición, para los riesgos de nivel **medio y alto** 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 Entidad y los riesgos con niveles de exposición **muy alto** se **debe** implementar planes de contingencia para responder a los riesgos materializados.

En esta etapa se establecen medidas de control (Planes de Tratamiento), para los riesgos de niveles **medio, alto y muy alto**, cuyo objetivo es reducir el nivel probabilidad y/o impacto. En dichos planes se detallan las medidas de control propuestas, los plazos de implementación previstos para cada medida de control, detallando la fecha de Inicio y de fin, además el Órgano o Unidad Orgánica responsable de implementarlo.

El Dueño del riesgo debe coordinar con los Órganos que forman parte del proceso evaluado, con la finalidad de establecer las medidas de control del riesgo identificado que de acuerdo a sus competencias deben implementar.

Tratamiento de los Riesgos de Corrupción

Los Órganos de la Entidad en caso identifiquen riesgos de corrupción deben darle un tratamiento, implementando medidas de control.

Para el tratamiento de los riesgos de corrupción, además de los controles existentes se deben tener en cuenta como mínimo los controles establecidos en la NTP - ISO 37001:2017.

Tratamiento de los Riesgos de Seguridad de la Información

Para el tratamiento de los riesgos de seguridad de la información deben emplear como mínimo los controles del Anexo A de la NTP- ISO/IEC 27001:2014.

Actividades para el Tratamiento del Riesgo en el proceso

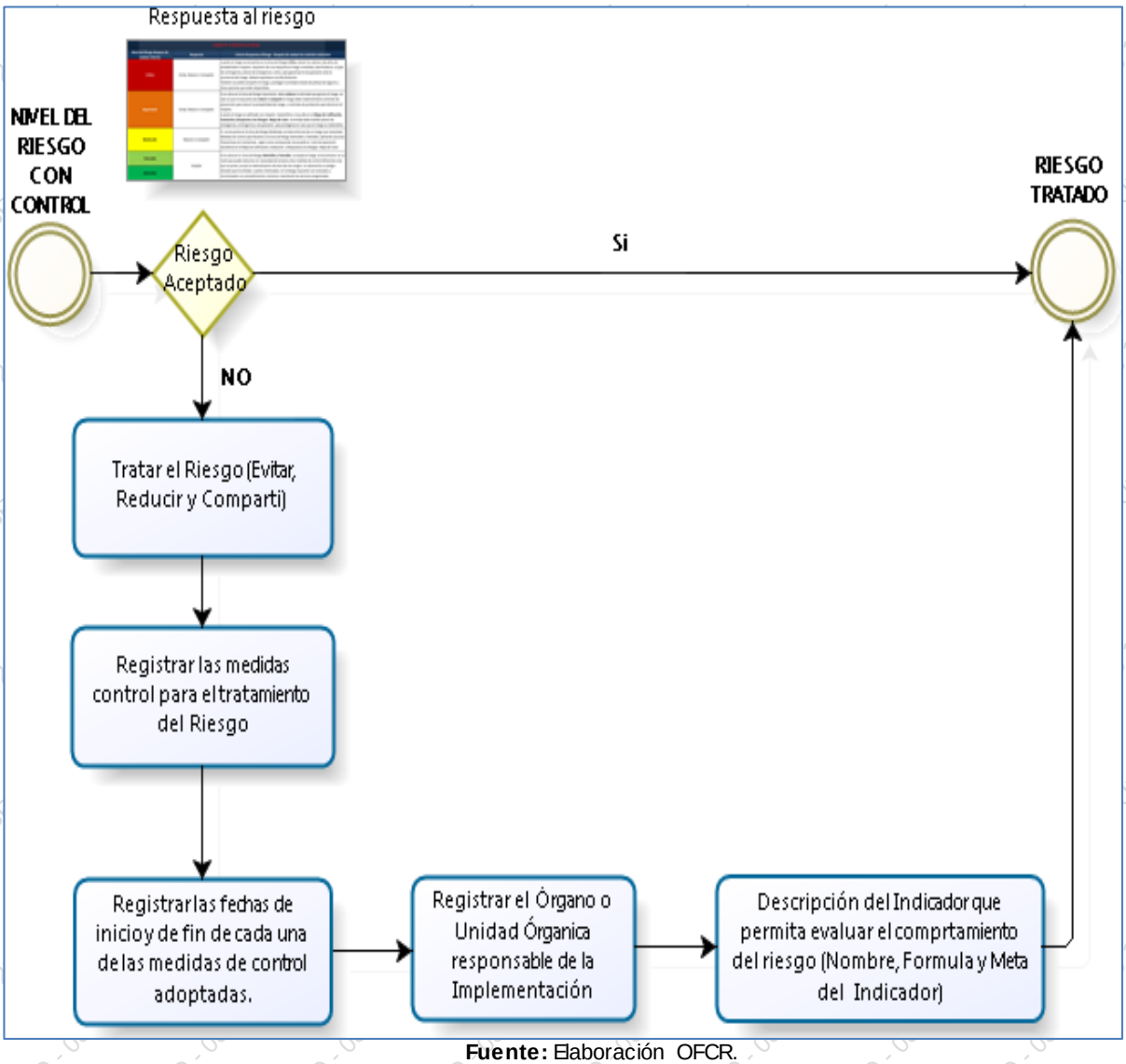
Las actividades que **debe** realizar el Gestor Líder de Riesgos y el Equipo de Riesgos en la etapa de tratamiento del riesgo en su proceso, serán las siguientes:

Nº de Actividad	Descripción de la actividad
13	Seleccionar la respuesta al riesgo para lo cual debe utilizar la **Tabla N° 15 Tipos de Respuesta al Riesgo - Anexo Nº 02.**
14	Si la respuesta es Evitar, Reducir o Compartir de acuerdo a los criterios para respuesta al riesgo en la etapa de tratamiento contenidas en la **Tabla N° 16 Criterios para la Respuesta al Riesgo en la etapa de tratamiento - Anexo Nº 02**, se deberán registrar las medidas de control para el tratamiento del riesgo identificado, los plazos y Órgano responsable de su implementación.

15	Describir un indicador relevante del proceso alineado al riesgo identificado, que permita medir el comportamiento del riesgo y la efectividad del control.

Como resultado de estas actividades se **debe** obtener las medidas de control para tratar el riesgo identificado contenido en el **Registro Nº 2: Plan de Acción Anual – Medidas de Control o Plan de Gestión Integral del Riesgo del Anexo Nº 02**.

Gráfico N° 7: 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 "Medidas de Control", se deben registrar las medidas de control que se propongan para el tratamiento al riesgo, luego de haberse efectuado el análisis y valoración del riesgo identificado, asimismo se deben registrar los plazos (fecha de inicio y fin) para la implementación de las medidas de control.

En el campo Órgano o Unidad Orgánica se debe registrar el responsable de implementar las medidas de control propuestas.

Ejemplo:

RESPUESTA AL RIESGO (TABLA N° 09 Y 10)	MEDIDA DE CONTROL	PLAZO DE IMPLEMENTACIÓN		ÓRGANO O UNIDAD ÓRGANICA RESPONSABLE DE IMPLEMENTACION
		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.	9/09/2019 9/09/2019 9/09/2019	8/06/2020 3/02/2020 30/12/2019	GOR

EVITAR
REDUCIR
COMPARTIR

En esta etapa de tratamiento la respuesta **"Aceptar"** solo aparecerá en la lista cuando el nivel del riesgo sea **Bajo**, al ser seleccionada dicha respuesta, automáticamente se bloquearán los campos de: "Medidas de Control", "Plazo de Implementación" (fecha de inicio y fin) y "Órgano o Unidad Orgánica Responsable de Implementación".

RESPUESTA AL RIESGO (TABLA N° 09 Y 10)	MEDIDA DE CONTROL	PLAZO DE IMPLEMENTACIÓN		ÓRGANO O UNIDAD ÓRGANICA RESPONSABLE DE IMPLEMENTACION
		FECHA DE INICIO	FECHA DE FIN	
ACEPTAR				

ACEPTAR

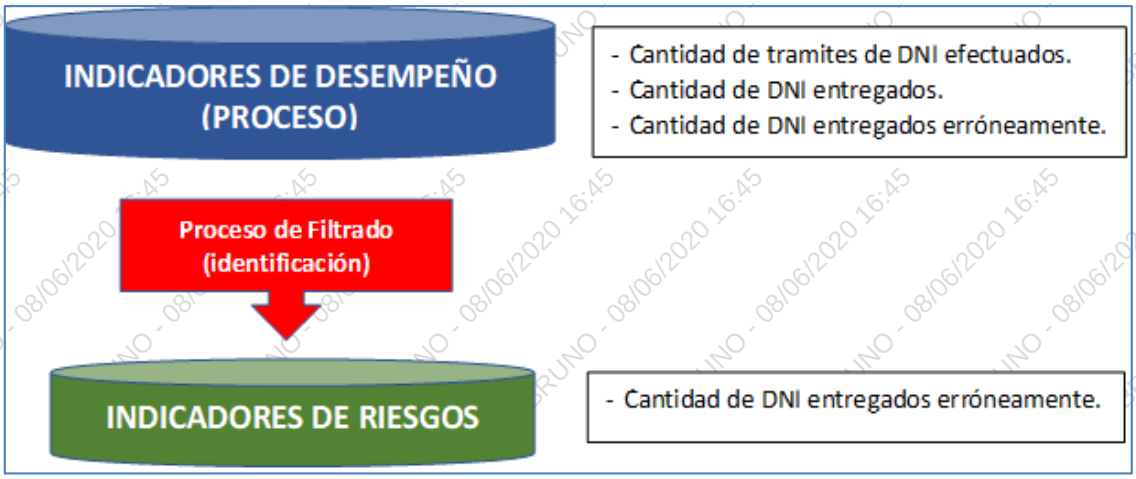
Formulación de Indicadores del Riesgo

Con la finalidad de medir la eficiencia de los controles existentes que mitigan el riesgo identificado, se debe establecer un indicador. Para ello, es importante considerar los indicadores de desempeño de los procesos que se encuentren directamente relacionados al riesgo, considerando las disposiciones establecidas por el Órgano técnico competente a cargo de la gestión por procesos.

El Dueño del Riesgo deberá establecer la meta del indicador de acuerdo a los niveles de

aceptación establecidos.

Gráfico N° 8: Indicadores



Fuente: Elaboración OFCR.

En el campo Indicador se debe describir: Nombre, fórmula y meta del indicador.

INDICADOR		
NOMBRE DEL INDICADOR DEL RIESGO	FÓRMULA DEL INDICADOR	META DEL INDICADOR
Porcentaje de DNI entregados a personas distinta al tiutular	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

- La medición del Indicador debe ser definida por el Dueño del Riesgo.

5.5 SEGUIMIENTO Y REVISIÓN

Es realizada por el Dueño del Riesgo y consiste en verificar si la ejecución de las medidas de control establecidas para el tratamiento de riesgos contenidos en el **Plan de Acción Anual - Medidas de Control o Plan de Gestión Integral del Riesgo del Anexo N° 02** de los productos (priorizados y no priorizados) se están implementando de acuerdo a lo planificado. Asimismo, evalúa el cumplimiento y la eficacia de la implementación de las medidas de control o tratamiento del riesgo.

Es importante precisar que pocos riesgos permanecen estáticos. Por lo tanto, los riesgos y la efectividad de sus medidas de control necesitan ser sometidos a seguimiento permanente por el Dueño del Riesgo para asegurar que circunstancias cambiantes no alteren los objetivos del proceso o producto.

- Las actividades desarrolladas en esta etapa se encuentran a cargo del Dueño del Riesgo a través del Gestor Líder de Riesgos para ello se debe realizar lo siguiente:

a) El seguimiento al avance de implementación del Plan de Acción Anual - Medidas de Control o Plan de Gestión Integral del Riesgo de los productos (priorizados y no priorizados) incluida la eficacia de las medidas de control establecidos.

b) Analizar los cambios en el contexto externo – interno con la finalidad de identificar nuevos riesgos o cambios en el nivel de exposición.

c) Efectuar la revisión y reportar mediante un informe trimestral a la Secretaria General el avance del Plan de Acción Anual -Medidas de Control o Plan de Gestión Integral del Riesgo de los productos (priorizados y no priorizados).

d) Reportar mediante un informe semestral a la Secretaria General, el avance consolidado de los resultados de las medidas de control implementadas dentro del Plan de Acción Anual - Medidas de Control o Plan de Gestión Integral del Riesgo de los productos (priorizados y no priorizados).

Actividades para el Seguimiento y Revisión del Riesgo

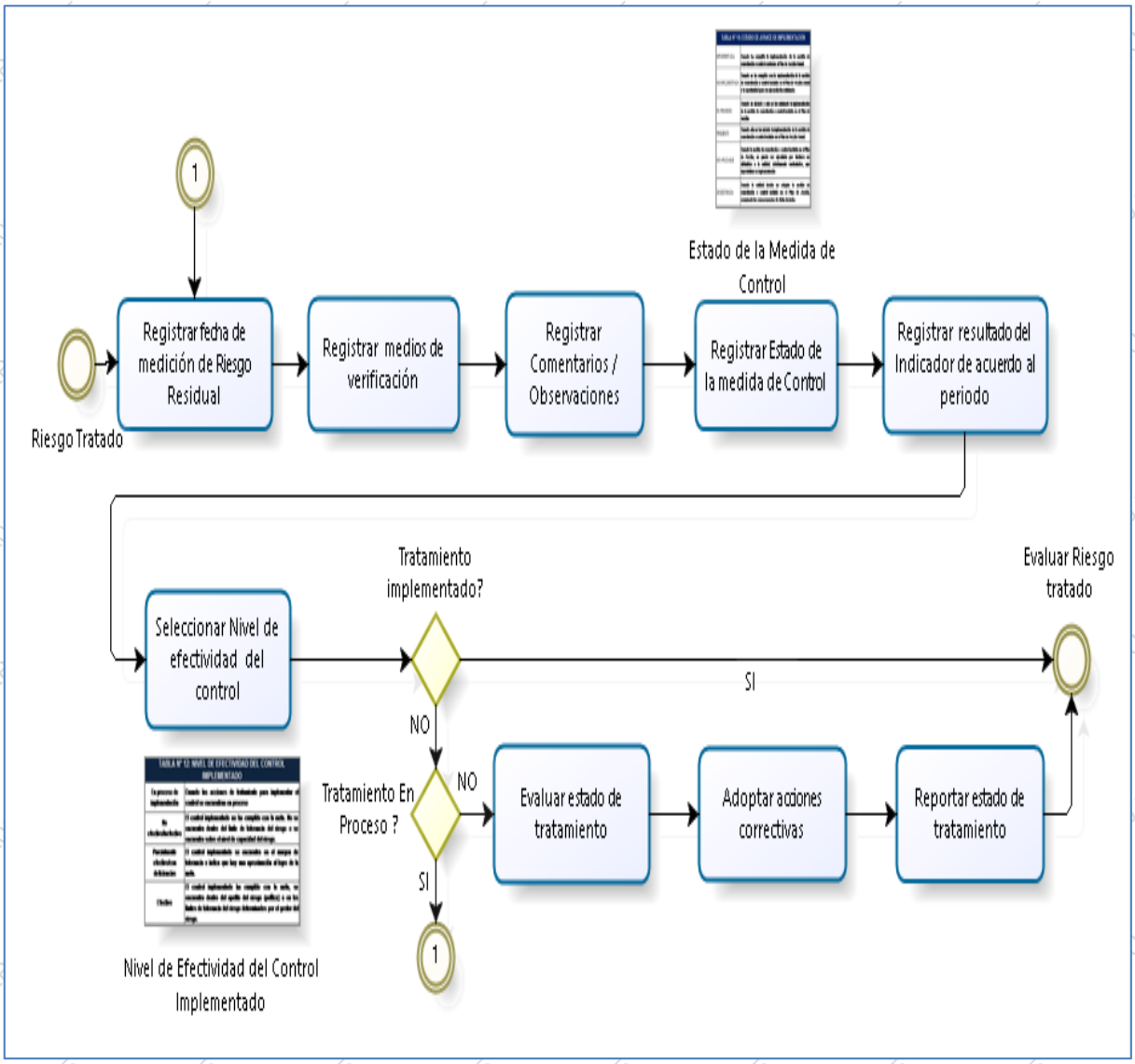
Las actividades que debe realizar el Gestor Líder de Riesgos y el Equipo de Riesgos en la etapa de Seguimiento y Revisión durante el avance de implementación de las acciones del tratamiento del riesgo en su proceso, serán las siguientes:

N° de Actividad	Descripción de la Actividad
16	Registrar la fecha de medición del riesgo residual, la cual debe realizarse a los tres meses después de haber culminado su implementación.
17	Registrar los medios de verificación que sustentan la implementación de las acciones ejecutadas (Evidencias).
18	Registrar Comentarios y Observaciones sobre las acciones ejecutadas (de corresponder)
19	Seleccionar el estado de avance de implementación de la medida de control, considerando la Tabla N° 17 Estado de Avance de Implementación del Anexo N° 02.
20	Registrar el resultado del indicador (Los responsables definirán su periodicidad de Registro, considerando para ello los plazos de implementación de las medidas de control) ello permitirá ver su comportamiento.
21	Seleccionar el nivel de efectividad de acuerdo al resultado del indicador para lo cual se debe utilizar la Tabla N° 18 Nivel de Efectividad del Control Existente/ Implementado del Anexo N° 02.

Como resultado de estas actividades obtenemos el nivel de efectividad de las medidas de control que se vienen implementando.

Gráfico N° 9: Seguimiento y Revisión

Estado de avance de implementación de las acciones adoptadas para el tratamiento del riesgo - evaluación del indicador



Fuente: Elaboración OFCR.

Continuando con el caso, en la etapa de Seguimiento y Revisión se registra la fecha de medición del riesgo residual la cual se estableció, luego de haber trascurrido tres meses de haber implementado las medidas de control; se registra el estado de avance de la implementación de las medidas de control para el tratamiento del Riesgo, así mismo se registran los medios de verificación que sustentan el avance, comentarios u observaciones necesarios para precisar las acciones ejecutadas, se selecciona el estado de la medida de control de acuerdo a su nivel de implementación, de igual forma se registra el resultado que muestra la evaluación del indicador y se selecciona el nivel de efectividad del control.

Ejemplo:

SEGUIMIENTO Y REVISION					
FECHA DE MEDICIÓN DEL RIESGO RESIDUAL	ESTADO DE AVANCE DE IMPLEMENTACIÓN DE LAS MEDIDAS DE CONTROL ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO			EVALUACIÓN DEL INDICADOR	
	MEDIOS DE VERIFICACION	COMENTARIOS U OBSERVACIONES	ESTADO DE LA MEDIDA DE CONTROL (TABLA N° 17)	RESULTADO DEL INDICADOR	NIVEL DE EFECTIVIDAD DEL CONTROL (TABLA N° 18)
1/10/2020	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. 3. Solicitud de actualización de plan Capacitación para los servidores que laboran en la Agencias y Oficinas.	1. Se ha efectuado el requerimiento presupuestal a GPP para gestionar el requerimiento. 2. Se esta efectuando la revisión interna a cargo de las uuoo de la GOR. 3. Se ha requerido incorporar capacitaciones sobre el proceso de captura y entrega del DNI.	EN PROCESO	0.01%	EN PROCESO DE IMPLEMENTACION

IMPLEMENTADA
NO IMPLEMENTADA
EN PROCESO
PENDIENTE
NO APLICABLE
DESESTIMADA

5.5.1 Cambios y Modificaciones en el Plan de Acción Anual – Medidas de Control (PAAMC)

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

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

b) De identificarse nuevos riesgos, por cambios en el entorno externo/interno se deberán incorporar en el PAAMC, informando a la SGEN.

c) Coordinar con los responsables de otros Órganos participantes de las medidas de control para cumplir con los plazos establecidos en el tratamiento de los riesgos identificados.

d) Reportar a la SGEN, el PAAMC o Plan de Gestión Integral del Riesgo modificado, justificando las razones de los cambios, quien a su vez remitirá al Titular de la Entidad para su aprobación.

5.5.2 Evaluación del Control Implementado para Obtener el Riesgo Residual

Luego de implementar las medidas de control para tratar los riesgos en el periodo programado, se debe evaluar el resultado para obtener el Riesgo Residual, con la finalidad de establecer si las acciones implementadas han permitido llevar al riesgo a los niveles aceptados por la Entidad.

En el caso de los Riesgos de Seguridad de la Información se aplicará lo dispuesto a la normativa existente relacionada a la Gestión de la Efectividad de Controles de Seguridad de la Información a cargo de la OSDN.

Las actividades que deben realizar el Gestor Líder de Riesgos y el Equipo de Riesgos en la etapa de Seguimiento y Revisión para obtener el Riesgo Residual en su proceso, son las siguientes:

Nº de Actividad	Descripción de la actividad
22	Registrar el o los controles implementados según corresponda, para lo cual debe utilizar el Registro N°3: Evaluación de Controles existente/implementados del Anexo N° 02.
23	En el Registro N°3: Evaluación de Controles existente/implementados del Anexo N° 02 se debe realizar lo siguiente: 23.1. Registrar el código del control del riesgo. 23.2. Seleccionar el tipo de control, para lo cual debe utilizar la Tabla N° 12 Tipos de Control Existente/implementado - Anexo Nº 02. 23.3. 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**?** 23.4. Calificar el control o controles existente/implementado de acuerdo a la Tabla N° 13: Criterios para el Análisis del Control Existente/implementado - Anexo Nº 02. 23.5. Seleccionar el control con mayor nivel de efectividad de acuerdo a la Tabla N° 14 Rangos del resultado de la calificación del control existente / implementado – Anexo N° 02 (*). 23.6. Trasladar los datos del control seleccionado al Registro N° 2: Plan de Acción Anual - Medidas de Control o Plan de Gestión Integral del Riesgo del Anexo N° 02 en la etapa Tratamiento, Seguimiento y Revisión del Riesgo, 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 obtiene el Riesgo Residual.

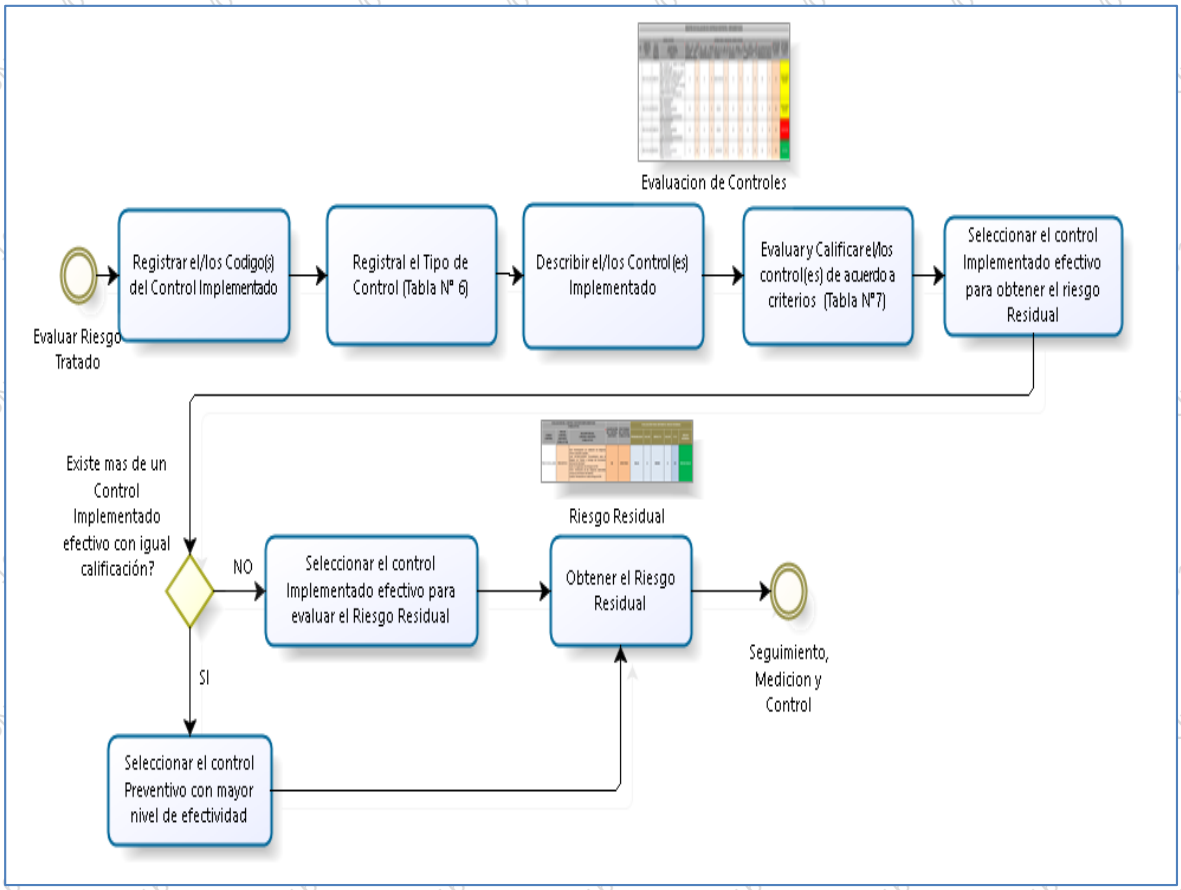
a) En el caso que el **Riesgo Residual** no haya permitido llevar el riesgo a los niveles aceptados por la Entidad, el Dueño del Riesgo del producto (priorizado y no priorizado) de los procesos definidos por la Entidad, conjuntamente con el Gestor Líder de Riesgos y el equipo de Riesgos deben evaluar lo siguiente:

- La eficacia y eficiencia de las medidas de control implementadas.
- El costo beneficio de adoptar nuevas medidas de control para su tratamiento.

b) Realizada la evaluación se deben adoptar las medidas de control necesarias para continuar gestionando los riesgos.

c) Si las opciones para el tratamiento no disminuyen el nivel de exposición al riesgo de acuerdo a los criterios establecidos por la Entidad, éste debería ser ACEPTADO, manteniéndose en continuo seguimiento y revisión, reportando a la SGEN para su evaluación.

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



Fuente: Elaboración OFCR.

Continuando con el ejemplo. Una vez implementadas las medidas de control, se procederá a efectuar nuevamente la evaluación del o los controles implementados. Para ello, se utiliza el "Registro N° 3 - Evaluación de Controles Existentes/Implementados" y las Tablas N° 12, N° 13 y N° 14 del anexo N° 02.

Ejemplo:

ITEM	CODIGO DEL CONTROL DEL RIESGO	CONTROL EXISTENTE / IMPLEMENTADO	
		TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE / IMPLEMENTADO
4	P08.01.03.03_C004	PREVENTIVO	**Qué:** Homologación y/o validación de imágenes (firma e impresión dactilar) **Cuál:** GP-269-G0R/005 "Procedimiento para el Registro 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. **ándo:** Permanente en cada entrega de DNI.

SIN CONTROLES
PREVENTIVO
CORRECTIVO

CRITERIOS PARA LA EVALUACIÓN DEL CONTROL EXISTENTE/IMPLEMENTADO												CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA N° 14)
¿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?			
SI	20	SI	10	SEMIAUTOMATICO	10	SI	10	SI	25	SI	20	95	EFECTIVO

- Cuando se implemente más de una medida de control y se obtenga 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.

El resultado de la evaluación del control se traslada al Registro N° 2: PAAMC o Plan de Gestión Integral del Riesgo del Anexo N° 02 en la etapa Tratamiento, Seguimiento y Revisión del Riesgo**,** con ello se efectuará la evaluación del Riesgo Residual.

FECHA DE MEDICIÓN DEL RIESGO RESIDUAL	ESTADO DE AVANCE DE IMPLEMENTACIÓN DE LAS MEDIDAS DE CONTROL ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO			EVALUACIÓN DEL INDICADOR	
	MEDIOS DE VERIFICACION	COMENTARIOS U OBSERVACIONES	ESTADO DE LA MEDIDA DE CONTROL (TABLA N° 17)	RESULTADO DEL INDICADOR	NIVEL DE EFECTIVIDAD DEL CONTROL (TABLA N° 18)
1/10/2020	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. 3. Solicitud de actualización de plan Capacitación para los servidores que laboran en la Agencias y Oficinas.	1. Se ha efectuado el requerimiento presupuestal a GPP para gestionar el requerimiento. 2. Se esta efectuando la revisión interna a cargo de las uuoo de la GOR. 3. Se ha requerido incorporar capacitaciones sobre el proceso de captura y entrega del DNI.	EN PROCESO	0.01%	NO EFECTIVO

SEGUIMIENTO Y REVISION											
EVALUACION DEL CONTROL EXISTENTE/IMPLEMENTADO			CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA N° 14)	EVALUACIÓN PARA OBTENER EL RIESGO RESIDUAL					
CODIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA N° 13)			PROBABILIDAD (TABLA N° 7)	VALOR	IMPACTO (TABLAS N° 8, 9, 10, Registro 6)	VALOR	P X I	NIVEL DE EXPOSICIÓN (RIESGO RESIDUAL) (TABLA N° 11, 23)
P08.01.03.03_C004	PREVENTIVO	Qué: Homologación y/o validación de imágenes (firma e impresión dactilar) Cuál: GP-269-GOR/005 "Procedimiento para el Registro 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.	95	EFECTIVO	MEDIA	6	BAJO	4	24	RIESGO BAJO

Luego de la evaluación del control implementado, se debe tener en cuenta el control de mayor efectividad para obtener el Riesgo Residual. En el presente ejemplo, se observa que

se ha reducido la probabilidad y el impacto, llevando al riesgo residual a un nivel de **RIESGO BAJO**.

			IMPACTO			
			BAJO	MEDIO	ALTO	MUY ALTO
			4	6	8	10
PROBABILIDAD	MUY ALTA	10	40 RIESGO MEDIO	60 RIESGO ALTO	80 RIESGO MUY ALTO	100 RIESGO MUY ALTO
	ALTA	8	32 RIESGO MEDIO	48 RIESGO ALTO	64 RIESGO ALTO	80 RIESGO MUY ALTO
	MEDIA	6	24 RIESGO BAJO	36 RIESGO MEDIO	48 RIESGO ALTO	60 RIESGO ALTO
	BAJA	4	16 RIESGO BAJO	24 RIESGO BAJO	32 RIESGO MEDIO	40 RIESGO MEDIO

5.6 SEGUIMIENTO, MEDICIÓN Y CONTROL

Actividad permanente en el proceso de la Gestión Integral del Riesgo liderada por la OFCR, quien coordina con los integrantes del Equipo Técnico conformado por la Oficina de Seguridad y Defensa Nacional (OSDN), Gerencia de Calidad e Innovación (GCI), el Oficial de Seguridad de la Información (OSI), el Oficial de Cumplimiento del Sistema de Gestión Antisoborno (OCSGA), y otros que se asignen, para verificar y evaluar lo siguiente:

a) El PAAMC o Plan de Gestión Integral del Riesgo formulados por los Órganos responsables en la Entidad de productos (priorizado y no priorizado), así como los procesos que participan en el producto.

b) La implementación de las medidas de control contenidas en los PAAMC o Plan de Gestión Integral del Riesgo.

c) La eficacia de las medidas de control implementadas.

Para el desarrollo de estas actividades, la SGEN traslada el PAAMC o Plan de Gestión Integral del Riesgo de productos (priorizado y no priorizado) remitidos por los Órganos responsables a la OFCR, quien con la información recibida desarrolla las siguientes acciones:

- Verificar y evaluar el PAAMC o Plan de Gestión Integral del Riesgo de productos (priorizado y no priorizado), de acuerdo a los criterios formulados en el presente documento, teniendo en cuenta lo siguiente:

  a) El cumplimiento de los plazos establecidos para la implementación de las medidas de control.

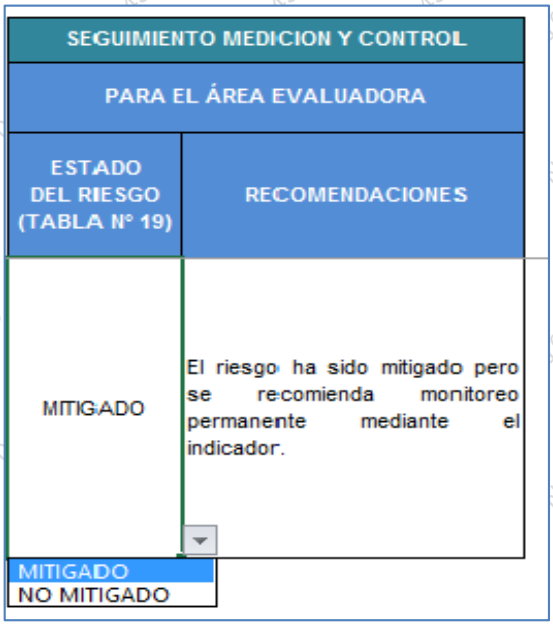
  b) El nivel de efectividad de las medidas de Control implementadas.

  c) La adopción de medidas correctivas cuando se presenten dificultades en su proceso de implementación o se haya identificado nuevos riesgos.

d) Si el riesgo identificado es de seguridad de la información, corrupción o proyectos, coordina con el o los integrantes del equipo técnico la verificación y evaluación correspondiente.

Continuando con el caso, la OFCR y/o el equipo técnico de la Gestión Integral del Riesgo, registrará en el campo RECOMENDACIONES la información correspondiente según corresponda el tipo de riesgo a evaluar, en el Registro N° 2: PAAMC o Plan de Gestión Integral del Riesgo del Anexo N° 02 en la etapa Tratamiento, Seguimiento y Revisión del Riesgo.

Ejemplo:



Luego de la evaluación, se observa que el riesgo se encuentra MITIGADO. Sin embargo, se ha recomendado acciones permanentes de monitoreo a cargo del Órgano responsable.

5.7 COMUNICACIÓN Y CONSULTA

El propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como el derecho a la privacidad de las personas.

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 Entidad, así como la recepción, documentación y respuesta a las comunicaciones de origen externo, alineada al modelo de gestión documental de la Directiva DI-424-SGEN/OAD/004 "Modelo De Gestión Documental del RENIEC" y la DI-417-SGEN/010 “Gestión Documental del RENIEC”.

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

Cuadro N° 1: 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 Micro sitio de Control Interno Inducción a personal nuevo. SITD	GPP/SGRM GII GTH ER
Directiva 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 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

Los reportes que realizan los Órganos en el proceso de la Gestión Integral del Riesgo.

Cuadro N° 2: Flujo de Comunicación Interna

¿Qué se debe comunicar?	¿Dónde se genera la información?	¿Quién debe comunicar?	¿A quién?	¿Cómo?	¿Cuándo?	Resultado
Reporte de Eventos de perdida (Reg. 1.1) e Incidentes de Seguridad de la Información consolidado	Procesos	Dueño del Riesgo.	GG, SGEN, OSDN CC. OFCR, Oficial de Seguridad de la Información (OSI) y Oficial de Cumplimiento del Sistema de Gestión Antisoborno (OCSGA)	SITD	Mensual	Registro de Eventos de Pérdida
PAAMC o Plan de Gestión	Procesos	Gestor Líder de Riesgos.	Dueño del Riesgo	SITD	Al séptimo mes y al	PAAMC o Plan de Gestión

Integral del Riesgo de los Productos priorizados y no priorizados)					cierre del año	Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo
PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo	Procesos	Dueño del Riesgo	SGEN, GG. CC. OFCR CC. OSDN CC. OSI CC. OCSGA CC. GCI	SITD	Al séptimo mes y al cierre del año	PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo
PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo	Procesos (Consolidado PAA Institucional por el Equipo Técnico GIR)	OFCR	SGEN, GG. CC. OSDN CC. OSI CC. OCSGA CC. GCI	SITD	Al séptimo mes y al cierre del año	PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional visado por SGEN
PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional visado por SGEN	Procesos	SGEN	Jefatura Nacional (JNAC)	SITD	Al séptimo mes y al cierre del año	PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional aprobado por JNAC

PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional aprobado por JNAC	Procesos	JNAC	Órganos y Unidades Orgánicas	SITD	Al séptimo mes y al cierre del año	PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional aprobado por JNAC y difundido.

Los reportes que realiza la Entidad al Órgano de Control Gubernamental de la Gestión Integral del Riesgo dentro del Plan de Acción Anual – Medidas de Control.

Cuadro N° 3: Flujo de Comunicación Externa

¿Qué se debe comunicar?	¿Dónde se genera la información?	¿Quién debe comunicar?	¿A quién?	¿Cómo?	¿Cuándo?	Resultado
PAAMC o Plan de Gestión Integral del Riesgo de los Productos priorizados y no priorizados) Aprobado por el Dueño del Riesgo consolidado institucional aprobado por JNAC	JNAC	JNAC	CGR	Aplicativo Web SCI - CGR	Al séptimo mes y al cierre del año	PAAMC aprobado por JNAC

5.8 REGISTRO E INFORME

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

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

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

Para el tratamiento de las oportunidades se debe priorizar aquellas que luego de ser evaluadas se encuentren en los niveles de exposición **"Alto"** y **"Muy Alto**". Asimismo, se deben considerar los riesgos asociados.

Para identificar, analizar, valorar y tratar las oportunidades se debe utilizar el Registro N° 6: Plan de Gestión de Oportunidades del Anexo N° 06 y las tablas contenidas en el Anexo N° 07.

VI. VIGENCIA

El presente Manual entra en vigencia a partir de su aprobación.

VII. APROBACIÓN

Mediante Resolución Secretarial.

IX. ANEXOS

ANEXO N° 01

REGISTRO N°1: REPORTE DE EVENTOS DE PÉRDIDA				
1. DATOS GENERALES				
Sede/Instalación/Oficina:				
Proceso Afectado:				
Producto afectado:				
Fecha:		**Hora:**		
Reportado por:			**Cargo:**	
2. REGISTRO				
Descripción del Evento de Pérdida:				
Tipo de Evento de pérdida:				
Categoria de Evento de pérdida:				
Efectos del Evento de pérdida:				
Respuesta al Evento de pérdida:				

REGISTRO N°1.1: REGISTRO DE EVENTOS DE PÉRDIDA

Órgano/Unidad Orgánica:											FECHA DE REPORTE:			
Nº	Fecha de ocurrencia:	Lugar de Ocurrencia	Dependencia	Producto	Proceso, actividad o tarea afectado	Tipo de Incidente / Evento de pérdida	Categoria de Incidente / Evento de pérdida	Descripción de la Incidente / Evento de Pérdida	Causas	Efectos del Incidente / Evento de pérdida	Respuesta al Incidente/Evento de pérdida	Fecha de implementación	Acciones de Seguimiento	Estado

Firma del Gerente

Firma del responsable de implementación

TABLA N° 1: TIPOS DE EVENTOS DE PÉRDIDA POR RIESGOS			
TIPO	**DEFINICION**	**CATEGORIA**	**EJEMPLOS**
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas institucionales en las que se encuentra implicado, al menos, un servidor de la entidad.	Actividades no autorizadas	Aprobaciones y cancelaciones irregulares de trámite de DNI para beneficio de terceros.
		Robo y fraude	Robo de bienes,materiales y equipos, malversación, falsificación, soborno.
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación, suplantación.
Clientes, productos y Gestión Institucional	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación legal frente al cliente ciudadano.	Procedimientos Institucionales improcedentes	Cancelaciones que afecten los derechos a la identidad e identificación del ciudadano.
		Productos defectuosos	Productos no conformes, (productos que no cumplen con la caracteristicas de conforme).
		Selección de grupos de interés	Deficiencias en la investigación a provevedores, socios estratégicos, etc.
		Conflictos de interés	Favoritismo, uso inadecuado del poder para beneficio propio.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y/u otros causados por la mano del hombre	Pérdidas por desastres naturales u ocasionado por la mano del hombre (incendios), pérdidas humanas por causas externas (terrorismo, vandalismo).
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Errores en los tramites de la entidad, incumplimiento de plazos, errores administrativos y financieros.
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

ANEXO N° 02

REGISTRO N° 2: PLAN DE ACCION ANUAL - MEDIDAS DE CONTROL / PLAN DE GESTION INTEGRAL DEL RIESGO

IDENTIFICACION, ANALISIS Y VALORACIÓN DEL RIESGO

Fecha: | Elaborado por: | Aprobado por:
Version: | Revisado por:

IDENTIFICACION DEL PROCESO Y PRODUCTO							IDENTIFICACIÓN DEL RIESGO								
PROCESO NIVEL 1	CÓDIGO DEL PROCESO DEL NIVEL DESAGREGADO (*)	PROCESO NIVEL DESAGREGADO (*)	OBJETIVO DEL PROCESO	ÓRGANO RESPONSABLE DEL PROCESO	PRODUCTO PRIORIZADO	CÓDIGO DEL RIESGO	HECHO O AMENAZA (Para Riesgos de Seguridad de la información y Desastres)	DESCRIPCIÓN DEL RIESGO	CAUSAS O VULNERABILIDAD	EFECTOS	CÓDIGO DE ACTIVOS DE INFORMACIÓN RELACIONADOS (REF. INVENTARIO DE ACTIVOS)	TIPO DE RIESGO (TABLA N° 4)	CATEGORIA DEL RIESGO (CORRUPCION/ PROYECTOS) (TABLA N° 5, 23)	FUENTE QUE ORIGINA EL RIESGO (TABLA N° 6)
Proceso de Identificación	PM01.01.01.03	Entrega de DNI	Entregar el DNI a los ciudadanos los cumpliendo los procedimientos establecidos.	GOR	Población cuenta con DNI (convencional)	P01.01.01.03_R01		Debido a las 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.	♦ Desconocimiento del procedimiento en la entrega de DNI por falta de capacitación. ♦ Incumplimiento del procedimiento. ♦ GP-269-GGR/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 biometricos 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.		OPERATIVO		INTERNA

REGISTRO N° 2: PLAN DE ACCION ANUAL - MEDIDAS DE CONTROL / PLAN DE GESTION INTEGRAL DEL RIESGO

IDENTIFICACION, ANALISIS Y VALORACIÓN DEL RIESGO

CALCULO DE LA PROBABILIDAD	ANALISIS Y VALORACION DEL RIESGO																								
	CRITERIOS DE IMPACTO (TABLA N° 9)										EVALUACION DEL CONTROL EXISTENTE / IMPLEMENTADO							NIVEL DEL RIESGO CON CONTROL						
PROBABILIDAD (TABLA N° 7)	VALOR	PARA LOS RIESGOS DE PROYECTO (TABLA N° 10)	SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL (TABLA N° 9)	CORRUPCION (REGISTRO N° 5)	OBJETIVOS ESTRATEGICOS INSTITUCIONALES	CUMPLIMIENTO LEGAL Y NORMATIVO	IMAGEN INSTITUCIONAL	OPERATIVIDAD	IMPACTO (TABLAS N° 8, 9, 10, Registro 9)	VALOR	CODIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA N° 13)	CALIFICACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL ACTUAL (TABLA N° 14)	PROBABILIDAD (TABLA N°7)	VALOR	IMPACTO (TABLAS N° 8, 9, 10, Registro 9)	VALOR	P X I	NIVEL DE EXPOSICIÓN DEL RIESGO (TABLA N° 11)	ACCION A REALIZAR
ALTA	8				MEDIO	BAJO	MEDIO	BAJO	MEDIO	6	R08.01.03.03_C001	PREVENTIVO	Qué: Homologación y/o validación de imágenes (firma e impresión dactar) Cuándo: Durante el proceso de "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.	55	NO EFECTIVO	ALTA	8	MEDIO	6	48	RIESGO ALTO	EL RIESGO DEBE SER TRATADO

REGISTRO Nº 2: PLAN DE ACCION ANUAL - MEDIDAS DE CONTROL / PLAN DE GESTION INTEGRAL DEL RIESGO

TRATAMIENTO - SEGUIMIENTO Y REVISION DEL RIESGO

Fecha:		Elaborado por:		Aprobado por:	
Version:		Revisado por:			

EXPOSICION DEL RIESGO EN EL PROCESO			TRATAMIENTO DEL RIESGO (DETERMINACION DE MEDIDA DE CONTROL)							
					PLAZO DE IMPLEMENTACIÓN			INDICADOR		
CÓDIGO DEL RIESGO	DESCRIPCIÓN DEL RIESGO	NIVEL DE EXPOSICIÓN DEL RIESGO (TABLA Nº 11,24)	RESPUESTA AL RIESGO (TABLA Nº 15)	MEDIDAS DE CONTROL	FECHA DE INICIO	FECHA DE FIN	ÓRGANO O UNIDAD ÓRGANICA RESPONSABLE DE IMPLEMENTACION	NOMBRE DEL INDICADOR DEL RIESGO	FÓRMULA DEL INDICADOR	META DEL INDICADOR
P01.01.01.03_R01	Debido a las deficiencias en la verificación de la identidad durante la entrega del DNI de mayor de edad en los locales de atención, podria ocasionar que el documento nacional de identidad sea entregado a persona distinta del titular generando perjuicio al ciudadano por uso indebido.	RIESGO ALTO	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.	12/08/2019 12/08/2019 12/08/2019	08/06/2020 03/02/2020 30/12/2019	GOR	Porcentaje de DNI entregados a personas distinta al tiutular	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

REGISTRO Nº 2: PLAN DE ACCION ANUAL - MEDIDAS DE CONTROL / PLAN DE GESTION INTEGRAL DEL RIESGO

TRATAMIENTO - SEGUIMIENTO Y REVISION DEL RIESGO

SEGUIMIENTO Y REVISION																	SEGUIMIENTO MEDICION Y CONTROL	
FECHA DE MEDICIÓN DEL RIESGO RESIDUAL	ESTADO DE AVANCE DE IMPLEMENTACIÓN DE LAS MEDIDAS DE CONTROL ADOPTADAS PARA EL TRATAMIENTO DEL RIESGO			EVALUACIÓN DEL INDICADOR		EVALUACION DEL CONTROL EXISTENTE/IMPLEMENTADO			CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA Nº 14)	EVALUACIÓN PARA OBTENER EL RIESGO RESIDUAL						PARA EL ÁREA EVALUADORA	
	MEDIOS DE VERIFICACION	COMENTARIOS U OBSERVACIONES	ESTADO DE LA MEDIDA DE CONTROL (TABLA Nº 17)	RESULTADO DEL INDICADOR	NIVEL DE EFECTIVIDAD DEL CONTROL (TABLA Nº 18)	CODIGO DEL CONTROL DEL RIESGO	TIPO DE CONTROL (TABLA Nº 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE (TABLA Nº 13)			PROBABILIDAD (TABLA Nº 7)	VALOR	IMPACTO (TABLAS Nº 8, 9, 10, Registro 5)	VALOR	P X I	NIVEL DE EXPOSICIÓN (RIESGO RESIDUAL) (TABLA Nº 11, 24)	ESTADO DEL RIESGO (TABLA Nº 19)	RECOMENDACIONES
1/10/2020	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 Nº000152-2018/GOR/RENIEC. 3. Solicitud de actualización de plan Capacitación para los servidores que laboran en la Agencias y Oficinas.	1. Se ha efectuado el requerimiento presupuestal a GPP para gestionar el requerimiento. 2. Se esta efectuando la revisión interna a cargo de las uuoo de la GOR. 3. Se ha requerido incorporar capacitaciones sobre el proceso de captura y entrega del DNI.	EN PROCESO	0.01%	NO EFECTIVO	P08.01.03.03_C004	PREVENTIVO	Qué: Homologación y/o validación de imágenes (firma e impresión dactilar) Cuál: GP-269-GOR/005 "Procedimiento para el Registro 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.	95	EFECTIVO	MEDIA	6	BAJO	4	24	RIESGO BAJO	MITIGADO	El riesgo ha sido mitigado pero se recomienda monitoreo permanente mediante el indicador.

REGISTRO N° 3: EVALUACION DE CONTROLES EXISTENTES / IMPLEMENTADOS

ITEM	CODIGO DEL CONTROL DEL RIESGO	CONTROL EXISTENTE/ IMPLEMENTADO		CRITERIOS PARA LA EVALUACIÓN DEL CONTROL EXISTENTE/IMPLEMENTADO (Tabla N° 13)							CALIFICACIÓN DEL CONTROL EXISTENTE	EFECTIVIDAD DEL CONTROL (TABLA N° 14)
		TIPO DE CONTROL (TABLA N° 12)	DESCRIPCIÓN DEL CONTROL EXISTENTE / IMPLEMENTADO	¿Existe un medio documentado y vigente 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?			

TABLA N° 2: TÉCNICAS UTILIZADAS EN LA GESTIÓN DEL RIESGO		
ITEM	**HERRAMIENTA**	**DESCRIPCION**
1	Luvia o tormenta de ideas	Técnica cualitativa, efectiva para generar ideas nuevas.
2	Entrevistas estructuradas o semiestructuradas	Entrevistar a participantes experimentados e interesados en la materia de riesgos así como aquellos funcionarios involucrados en los principales procesos.
3	Delphi	Es un método para predecir el futuro utilizando expertos en el área a la cual pertenece el problema.
4	Analisis 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	Analisis de causa primordial (analisis de daño unico)	Centra su analisis en los factores internos y externos que han dado, o pueden dar lugar, a eventos negativos (riesgos).
8	Analisis 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	Analisis causa y efecto (Ishikaw a)	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	Indices 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	Analisis de costos/beneficios y cadena de valor	Esta técnica permite, nos da el enfoque visual del conjunto de actividades que abarca: la logistica 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.

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

TABLA N° 4: 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.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
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 forma en que se administra 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.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
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.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
IMAGEN	Relacionados con la percepción y la confianza por parte de los grupos de interés en la entidad.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
MEDIO AMBIENTE	Comprende aquellos riesgos que pueden ocasionar deterioro o daños al medioambiente.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
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.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*
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, si no también por garantizar la Confidencialidad Integridad y Disponibilidad de la información.	*Glosario - ISO27001*
SEGURIDAD Y SALUD EN EL TRABAJO	Comprende aquellos riesgos, que pueden ocasionar accidentes, enfermedades ocupacionales e incidentes peligrosos que pongan en riesgo la seguridad o salud de los trabajadores.	*Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo*
TECNOLÓGICO	Se asocia con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales y futuras, contribuyendo al cumplimiento de su misión.	*Adaptacion del marco COSO ERM Integrating with Strategy and Performance, y las dispociones de la CGR para ser aplicada en la presente metodología.*

TABLA N° 5: CATEGORIA DE RIESGOS DE PROYECTO		
CATEGORIA	**SUB CATEGORIA**	**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 fiabildad
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 softw are de planificación
	Control	Cambios constantes en los criterios para valorar el progreso
	Comunicación	Informes poco claros sobre la evolución del proyecto

TABLA N° 6: 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° 7: NIVELES DE PROBABILIDAD		
CLASIFICACION	**NIVEL**	**DESCRIPCION Y FRECUENCIA**
BAJA	4	El riesgo podría ocurrir rara vez sólo en circunstancias excepcionales o en un horizonte aproximado mayor a un año.
MEDIA	6	El riesgo puede ocurrir en algún momento relativamente frecuente o en un futuro cercano menor a un semestre.
ALTA	8	El riesgo puede ocurrir en la mayoría de las circunstancias o aproximadamente una vez al mes.
MUY ALTA	10	El riesgo podría ocurrir en la mayoría de las circunstancias en un presente muy cercano o aproximadamente en dias o semanas
Fuente: DI-006-2019-CG/INTEG -CGR		
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° 08: NIVELES DEIMPACTO PARA RIESGOS EN GENERAL					
Impacto	**Nivel**	**Objetivos Estratégicos Institucionales**	**Cumplimiento legal y normativo**	**Imagen institucional**	**Operatividad**
BAJO	4	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 auditorias, 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.
MEDIO	6	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 auditorias, 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.
ALTO	8	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 auditorias, 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.
MUY ALTO	10	Consecuencias afectan catastróficamente los resultados y objetivos institucionales.	Incumplimiento legal o normativo de impacto catastrófico. Hay graves multas o sanciones, observaciones-recomendaciones de auditorias, 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.

TABLA N° 9: NIVELES DE IMPACTO PARA RIESGOS EN SEGURIDAD DE LA INFORMACION						
Impacto	**Nivel**	**Seguridad de la Información y Seguridad Digital**	**Objetivos Estratégicos Institucionales**	**Cumplimiento legal y normativo**	**Imagen institucional**	**Operatividad**
BAJO	4	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 auditorias, 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.
MEDIO	6	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 auditorias, 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.
ALTO	8	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 auditorias, 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.
MUY ALTO	10	Las consecuencias afectan de manera critica 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 auditorias, 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.

TABLA N° 10: NIVELES DE IMPACTO PARA RIESGO EN PROYECTOS

Impacto	Nivel	Impactos para Riesgos de Proyectos	Objetivos Estratégicos Institucionales	Cumplimiento legal y normativo	Imagen institucional	Operatividad
BAJO	4	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 auditorias, 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.
MEDIO	6	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 auditorias, 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.
ALTO	8	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 auditorias, 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.
MUY ALTO	10	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 auditorias, 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.

TABLA N° 11: MAPA DE RIESGOS (PROBABILIDAD x IMPACTO)

			IMPACTO			
			BAJO	MEDIO	ALTO	MUY ALTO
			4	6	8	10
PROBABILIDAD	MUY ALTA	10	40 RIESGO MEDIO	60 RIESGO ALTO	80 RIESGO MUY ALTO	100 RIESGO MUY ALTO
	ALTA	8	32 RIESGO MEDIO	48 RIESGO ALTO	64 RIESGO ALTO	80 RIESGO MUY ALTO
	MEDIA	6	24 RIESGO BAJO	36 RIESGO MEDIO	48 RIESGO ALTO	60 RIESGO ALTO
	BAJA	4	16 RIESGO BAJO	24 RIESGO BAJO	32 RIESGO MEDIO	40 RIESGO MEDIO

Fuente: DI-006-2019-CG/INTEG

TABLA N° 12: TIPOS DE CONTROL EXISTENTE / IMPLEMENTADO	
PREVENTIVO	Actúan sobre las causas de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera barrera de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos. El control se aplica antes (Entradas) o durante la ejecución del proceso, generalmente antes de la entrega de los productos (Salidas). **DETECTIVOS** Se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas. Generalmente sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Constituyen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los funcionarios. El control se aplica durante la ejecución del proceso. Y, puede identificar pérdidas o malos productos (Salidas).
CORRECTIVO	No prevén que un evento suceda, pero permiten enfrentar la situación una vez se haya presentado. **PLANES DE CONTINGENCIA** Su objetivo es establecer medidas de control correctivas a través de planes de acción que protejan a la institución contra los impactos resultantes de los eventos de pérdida (activos materiales, resultados económicos, vidas humanas, etc.). Permiten el restablecimiento de los procesos o de sus actividades, después de ser detectada la ocurrencia de un evento de pérdida o no deseable, posibilitando la modificación de las causas que propiciaron su ocurrencia. Estos planes se establecen y se ponen en ejecución cuando los controles no operan y/o no son eficaces; permiten eliminar o mejorar factores que posibilitan los eventos de pérdida. Por lo general, actúan como controles de protección o correctivos, podrían implicar reprocesos.
SIN CONTROLES	Que no cuenta con controles.No existe control definido o implementado.

TABLA N° 13: CRITERIOS PARA EL ANÁLISIS DEL CONTROL EXISTENTE / IMPLEMENTADO		
PREGUNTAS	VALORES	JUSTIFICACION
¿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 vigentes y actualizados (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 éstos, 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	La frecuencia o periodicidad en la aplicación del control puede ser: • **Permanente:** El control se realiza durante todo el proceso, es decir, en todas o en sus principales actividades, durante todo el tiempo de operación necesario. • **Periódico:** El control se realiza transcurridas un número de actividades del proceso o transcurrido un tiempo determinado. Se repite a intervalos determinados de tiempo (por horas, semanal, mensual, trimestral, etc.). • **Ocasional:** El control se realiza en el proceso, cada vez que se solicita o se requiere.
¿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° 14: 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 0-69	0	PREVENTIVO CORRECTIVO	Se mantiene el riesgo.	NO EFECTIVO	El contol 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 70-89	1	PREVENTIVO CORRECTIVO	Si el Control es Preventivo la Probabilidad disminuye en un nivel. Si el Control es Correctivo el Impacto 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.
ENTRE 90-100	1	PREVENTIVO CORRECTIVO	Si el Control es Preventivo la Probabilidad y el impacto disminuye en un nivel. Si el Control es Correctivo la Probabilidad y el impacto disminuye en un nivel.	EFECTIVO	El control implementado ha cumplido con la meta, se encuentra dentro del apetito del riesgo (politica) o en los limites de tolerancia del riesgo determinados por el gestor del riesgo.

TABLA N° 15: TIPOS DE 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	No se realizan acciones para reducir la probabilidad o el impacto considerando el nivel de riesgo aceptado por la entidad o tambien se puede Aceptar el riesgo a fin de perseguir una oportunidad.

TABLA N° 16 CRITERIOS PARA LA RESPUESTA AL RIESGO EN LA ETAPA DE TRATAMIENTO		
NIVEL DE EXPOSICION	**RESPUESTAS**	**CRITERIO**
RIESGO MUY ALTO	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.
RIESGO ALTO	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 consideren el Plan de contingencia con las debidas aprobaciones. Se deben aplicar actividades de control y controles adecuados; se reportan a Alta Dirección.
RIESGO MEDIO	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.
RIESGO BAJO	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.

TABLA N° 17: ESTADO DE AVANCE DE IMPLEMENTACIÓN	
IMPLEMENTADA	Cuando ha cumplido con la implementación de la medida de remediación o control conforme al Plan de Acción Anual.
NO IMPLEMENTADA	Cuando no ha cumplido con la implementación de la medida de remediación o control incluida en el Plan de Acción Anual y la oportunidad para su ejecución ha culminado.
EN PROCESO	Cuando ha iniciado y aún no ha culminado la implementación de la medida de remediación o control incluida en el Plan de Acción.
PENDIENTE	Cuando aún no ha iniciado la implementación de la medida de remediación o control incluida en el Plan de Acción Anual.
NO APLICABLE	Cuando la medida de remediación o control incluida en el Plan de Acción, no puede ser ejecutada por factores no atribuibles a la entidad, debidamente sustentados, que imposibilitan su implementación
DESESTIMADA	Cuando la entidad decide no adoptar la medida de remediación o control incluida en el Plan de Acción, asumiendo las consecuencias de dicha decisión.

TABLA N° 18: NIVEL DE EFECTIVIDAD DEL CONTROL EXISTENTE/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° 19: 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° 03

TABLA N° 20: SITUACIONES SUCEPTIBLES DE RIESGOS DE CORRUPCIÓN

FINANCIERO / CONTABLE
• Inclusión de gastos no autorizados. • Inversiones de recursos públicos en organizaciones de dudosa solidez a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros importantes del presupuesto. • Inexistencia de archivos contables u otros sustentos requeridos por ley. • Gastos irregulares o sin sustento técnico autorizados-ejecutados en beneficio propio o a cambio de una retribución económica.

DE CONTRATACIÓN (COMO PROCESO O BIEN LOS PROCEDIMIENTOS LIGADOS A ESTE)
• Estudios técnicos - economicos previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación (Estableciendo necesidades inexistentes o aspectos que benefician a un proveedor (es) en particular). • Disposiciones establecidas en los terminos de referencia que dirigen los procesos hacia un un proveedor (es) en particular. • Adendas que cambian condiciones generales o específicas del proceso para favorecer a grupos determinados. • Falsear información para motivar la aplicación de exoneraciones extraordinarias contempladas en la ley. • No contar con los recursos necesarios para la debida supervisión y control de desempeño del proveedor. • Falta o no aplicación de las penalidades por los incumplimientos de los Proveedores en la prestación de bienes o servicios.

DE INFORMACIÓN Y DOCUMENTACIÓN
• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o procesos en una persona. • Ausencia de sistemas de información. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación. • Incumplimiento de normas legales sobre lucha anticorrupción (planes, politicas y otros)

DE INVESTIGACIÓN Y SANCIÓN
• Ausencia o debilidad de canales de comunicación. • Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo. • Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Pertubación intencional del procedimiento administrativo sancionador • Exceder las facultades legales en los fallos.

DE TRÁMITES Y/O SERVICIOS INTERNOS Y EXTERNOS
• Cobros asociados al trámite. • Influencia de tramitadores • Tráfico de influencias: (amiguismo, persona influyente). • Demorar su realización.

DE RECONOCIMIENTO DE UN DERECHO (EXPEDICIÓN DE LICENCIAS Y/O PERMISOS)
• Omitir procedimientos para autorizar permisos y/o licencias. • Ofrecer beneficios económicos para aligerar la expedición o para modificar informacion otorgar licencias y/o permisos. • Tráfico de influencias: (amiguismo, persona influyente).

DIRECCIONAMIENTO ESTRATÉGICO
• Concentración de autoridad o exceso de poder. • Extralimitarse o usurpar funciones. • Ausencia o mal uso de los canales de comunicación. • Favoritismo, discriminación, clientelismo.

TABLA N° 21: PREGUNTAS GUIA PARA IDENTIFICAR RIESGOS DE CORRUPCIÓN

¿Qué acciones, hitos o procesos del producto se encuentran expuestos a riesgos de corrupción (comisión de delitos contra la administración pública: cobro indebido, colusión, peculado, malversación, soborno, cohecho, tráfico de influencias, enriquecimiento ilícito, entre otros)?
¿En qué casos, un funcionario podría tener incentivos para solicitar o recibir un soborno (coima)?
¿Qué procesos estarían más relacionados a posibles abusos de poder o alteración de información de la gestión de la institución?

TABLA N° 22: CRITERIOS PARA IDENTIFICAR EL RIESGO DE CORRUPCIÓN

DESCRIPCION DEL RIESGO	ACCION U OMISION	USO DEL PODER	DESVIAR LA GESTION DE LO PUBLICO	BENEFICIO PRIVADO
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X
Si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción.				
Es importante precisar que en la descripción de los riesgos de corrupción deben concurrir todos los componentes establecidos en el Registro N° 05: Matriz de Definición del Riesgo de Corrupción.				
Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.				

TABLA N° 23: TIPOS DE CORRUPCION

ITEM	TIPO DE CORRUPCION	DESCRIPCION
1	COLUSIÓN	Concertación entre un empleado público y personas particulares en los procesos de contratación pública para defraudar al Estado.
2	PECULADO	Apropiación de los bienes del Estado por parte de los empleados públicos a su favor o de terceros, así como el uso indebido de los mismos para un fin distinto al que le corresponde
3	MALVERSACIÓN DE FONDOS	Uso distinto al que estaba destinado el dinero o bienes que administra el empleado público, afectando el servicio o la función pública encomendada.
4	SOBORNO	El soborno, o coima, es un acto de corrupción en el que se otorga o recibe una dádiva a cambio de un favor u omisión de las obligaciones a las que está sujeta el cargo. Esta es la forma más común y extendida de corrupción. Esta dádiva puede adoptar formas diversas: dinero en efectivo, transferencia de acciones, favores sexuales o promesas diversas (Anwar, 2006; UNODC, 2004).
5	COHECHO	El empleado público busca obtener u obtiene dinero u otro beneficio a cambio de realizar u omitir una conducta funcional.
6	TRÁFICO DE INFLUENCIAS	Invocación de influencias reales o simuladas ante un empleado público que conozca un caso judicial o administrativo, a cambio de recibir dinero u otro beneficio.
7	ENRIQUECIMIENTO ILÍCITO	Incremento de patrimonio del empleado público sin justificación en relación a sus ingresos legítimos.

REGISTRO N° 4: CRITERIOS PARA EVALUAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN

CÓDIGO DEL RIESGO:	

ITEM	PREGUNTA SI EL RIESGO DE CORRUPCION SE MATERIALIZA PODRIA…	RESPUESTA		VALIDACION
		SI	NO	
1	¿Afectar al grupo de funcionarios del proceso?			
2	¿Afectar el cumplimiento de metas y objetivos estratégicos de la entidad?			
3	¿Afectar el cumplimiento de misión de la entidad?			
4	¿Afectar el cumplimiento de la misión del sistema electoral?			
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?			
6	¿Generar pérdida de recursos económicos?			
7	¿Afectar la generación de los productos o la prestación de servicios?			
8	¿Afectar al acceso a la identidad e identificación de los ciudadanos?			
9	¿Generar intervención de los órganos de control oci cgr?			
10	¿Dar lugar al proceso sancionador?			
11	¿Dar lugar al proceso disciplinario?			
12	¿Dar lugar a denuncia ante el Ministerio Público?			
13	¿Dar lugar a denuncia penal?			
14	¿Generar pérdida de credibilidad en el sistema electoral?			
15	¿Ocasionar lesiones físicas o pérdida de vidas humanas?			
16	¿Afectar la imagen a nivel regional?			
17	¿Generar pérdida de información en la entidad?			
18	¿Afectar la imagen a nivel nacional?			
19	¿Generar daño ambiental?			
♦ Si responde afirmativamente de 1 a 11 preguntas el impacto es ALTO ♦ Si responde afirmativamente de 12 a 19 preguntas el impacto es MUY ALTO				

IMPACTO	NIVEL	DESCRIPCION
ALTO	8	Consecuencias afectan significativamente a la imagen de la entidad, son percibidas por los grupos de interés. Se originan sanciones administrativas por los entes de control (CGR), y/o denuncias penales a servidores y/o funcionarios.
MUY ALTO	10	Consecuencias afectan de manera catastrófica deteriorando la imagen institucional ante los grupos de interés. Genera destituciones de servidores y/o funcionarios y/o penas de carcel.

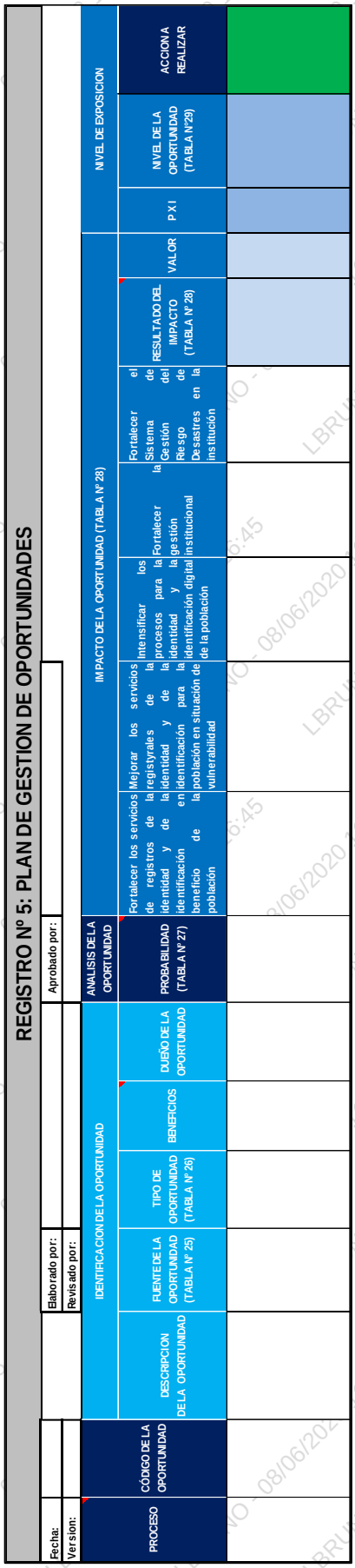
NOTA: Este registro debe ser firmado digitalmente por el dueño del riesgo identificado y archivado como evidencia para controles posteriores por los órganos competentes.

TABLA N° 24: MAPA DE RIESGOS DE CORRUPCION (PROBABILIDAD x IMPACTO)

			IMPACTO			
			BAJO	MEDIO	ALTO	MUY ALTO
			4	6	8	10
PROBABILIDAD	MUY ALTA	10	40 RIESGO MEDIO	60 RIESGO ALTO	80 RIESGO MUY ALTO	100 RIESGO MUY ALTO
	ALTA	8	32 RIESGO MEDIO	RIESGO ALTO	64 RIESGO ALTO	80 RIESGO MUY ALTO
	MEDIA	6	24 RIESGO BAJO	36 RIESGO MEDIO	48 RIESGO ALTO	60 RIESGO ALTO
	BAJA	4	16 RIESGO BAJO	24 RIESGO BAJO	32 RIESGO MEDIO	40 RIESGO MEDIO

No aplica para los riesgos de corrupción

ANEXO N° 04


REGISTRO Nº 5: PLAN DE GESTION DE OPORTUNIDADES
Fecha:
Version:
Elaborado por:
Revisado por:
Aprobado por:
PROCESO
CÓDIGO DE LA OPORTUNIDAD
IDENTIFICACION DE LA OPORTUNIDAD
DESCRIPCION DE LA OPORTUNIDAD
FUENTE DE LA OPORTUNIDAD (TABLA N° 25)
TIPO DE OPORTUNIDAD (TABLA N° 26)
BENEFICIOS
DUEÑO DE LA OPORTUNIDAD
ANALISIS DE LA OPORTUNIDAD
PROBABILIDAD (TABLA N° 27)
IMPACTO DE LA OPORTUNIDAD (TABLA N° 28)
Fortalecer los servicios de registros de la identidad y de identificación en beneficio de la población
Mejorar los servicios de la registros de la identidad y de 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
RESULTADO DEL IMPACTO (TABLA N° 28)
VALOR
NIVEL DE EXPOSICION
P X I
NIVEL DE LA OPORTUNIDAD (TABLA N°29)
ACCION A REALIZAR

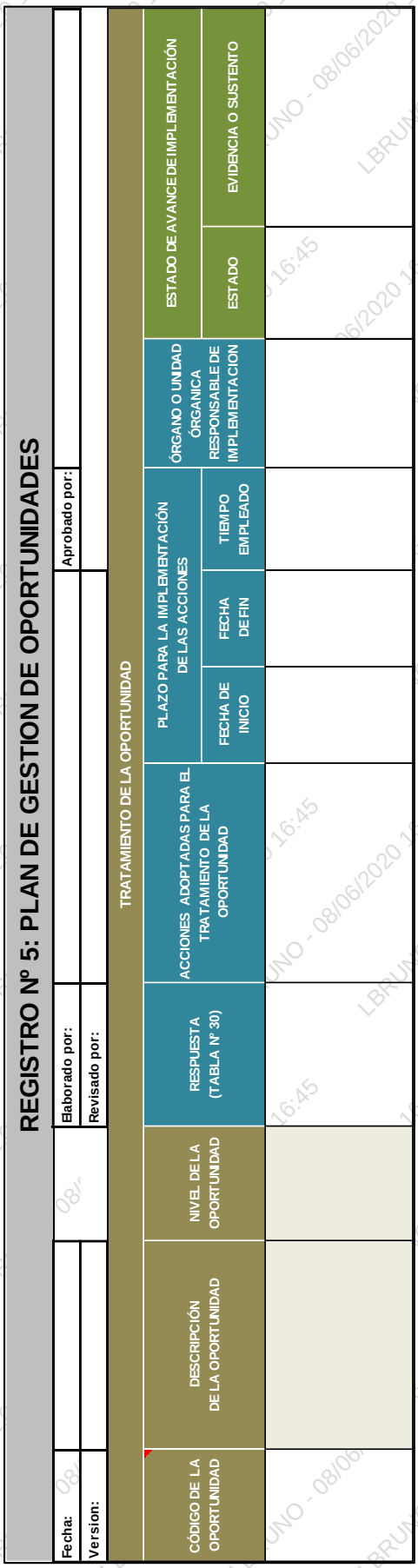

REGISTRO Nº 5: PLAN DE GESTION DE OPORTUNIDADES
Fecha:
Version:
Elaborado por:
Revisado por:
Aprobado por:
TRATAMIENTO DE LA OPORTUNIDAD
CÓDIGO DE LA OPORTUNIDAD
DESCRIPCIÓN DE LA OPORTUNIDAD
NIVEL DE LA OPORTUNIDAD
RESPUESTA (TABLA N° 30)
ACCIONES ADOPTADAS PARA EL TRATAMIENTO DE LA OPORTUNIDAD
PLAZO PARA LA IMPLEMENTACIÓN DE LAS ACCIONES
FECHA DE INICIO
FECHA DE FIN
TIEMPO EMPLEADO
ÓRGANO O UNIDAD ORGANICA RESPONSABLE DE IMPLEMENTACIÓN
ESTADO DE AVANCE DE IMPLEMENTACIÓN
ESTADO
EVIDENCIA O SUSTENTO

TABLA N° 25: FUENTE DE OPORTUNIDAD
INTERNA
EXTERNA

TABLA N° 26: TIPO DE OPORTUNIDAD
SERVICIOS
LEGALES
PERSONAS
TECNOLÓGICAS
GESTIÓN

TABLA N° 27: NIVELES DE PROBABILIDAD DE LA OPORTUNIDAD

Clasificación	Nivel	Oportunidad
MUY ALTA	10	La ocurrencia es inminente.
ALTA	8	**Probablemente se realice**.O se puede dar en el corto plazo.
MEDIA	6	**Puede ocurrir su realización**. O existen condiciones que hacen que la probabilidad de realización sea en el mediano plazo.
BAJA	4	**Podría realizarse.** O existen condiciones que hacen que su probabilidad de realización sea a largo plazo.

TABLA N° 28: CRITERIOS DE EVALUACIÓN DE IMPACTO DE LA OPORTUNIDAD

CLASIFICACION	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
BAJO	4	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.
MEDIO	6	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	8	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	10	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 impactoen 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° 29: MAPA DE LAS OPORTUNIDADES						
PROBABILIDAD	Muy Alta	10	MEDIO	ALTO	MUY ALTO	MUY ALTO
	Alta	8	MEDIO	MEDIO	ALTO	MUY ALTO
	Media	6	BAJO	MEDIO	MEDIO	ALTO
	Baja	4	BAJO	BAJO	MEDIO	MEDIO
			4	6	8	10
			Bajo	Medio	Alto	Muy alto
			IMPACTO			

TABLA Nº 30: 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 PRESENTEN LAS CONDICIONES PARA IMPLEMENTARLAS.

ANEXO N° 05

Registro N° 6: Reporte del Avance de la Gestión del Riesgo y oportunidades

Gerencia:

Fecha de Reporte:

Trimestre :

ITEM	PROCESO	PRODUCTO	ÓRGANO RESPONSABLE	CODIGO DEL RIESGO	RIESGO/OPORTUNIDAD	NIVEL DE EXPOSICION	RESPUESTA	MEDIDAS DE CONTROL	PLAZO PARA IMPLEMENTAR		NIVEL DE AVANCE				RESULTADO DEL INDICADOR	COMENTARIOS
									FECHA INICIO	FECHA FIN	% PROGRAMADO	% EJECUTADO	ESTADO			

* Considerar en el reporte para cada una de las medidas de control y/o acciones del tratamiento del riesgo/oportunidad adoptadas.

ANEXO N° 06

CUADRO DE CONTROL DE CAMBIOS DEL MGIR200-GG/OFCR/001 "GESTIÓN INTEGRAL DEL RIESGO"	
IDENTIFICACIÓN DEL CAMBIO	
Numeral Vigente	**Numeral Modificado**
I. OBJETIVO	I. OBJETIVO
II. ALCANCE	II. ALCANCE
III. REFERENCIAS NORMATIVAS	III. REFERENCIAS NORMATIVAS
Numeral 3.1	Numeral 3.1
Numeral 3.2	Numeral 3.2
Numeral 3.3	Numeral 3.3
Numeral 3.4	Numeral 3.4
Numeral 3.5	Numeral 3.5
Numeral 3.6	Numeral 3.6
Numeral 3.7	Numeral 3.7
Numeral 3.8	Numeral 3.8
Numeral 3.9	Numeral 3.9
Numeral 3.10	Numeral 3.10
Numeral 3.11	Numeral 3.11
Numeral 3.12	Numeral 3.12
Numeral 3.13	Numeral 3.13
Numeral 3.14	Numeral 3.14
Numeral 3.15	Numeral 3.15
Numeral 3.16	Numeral 3.16
Numeral 3.17	Numeral 3.17
Numeral 3.18	Numeral 3.18
Numeral 3.19	Eliminado
Numeral 3.20	Numeral 3.21
Numeral 3.21	Eliminado
Numeral 3.22	Numeral 3.24
Numeral 3.23	Numeral 3.25
Numeral 3.24	Eliminado
Numeral 3.25	Eliminado
Numeral 3.26	Numeral 3.27
Numeral 3.27	Numeral 3.34
Numeral 3.28	Numeral 3.33
Numeral 3.29	Eliminado
No existía en esta versión	Numeral 3.19
No existía en esta versión	Numeral 3.20
No existía en esta versión	Numeral 3.22
No existía en esta versión	Numeral 3.23
No existía en esta versión	Numeral 3.26
No existía en esta versión	Numeral 3.28
No existía en esta versión	Numeral 3.29

No existía en esta versión	Numeral 3.30
No existía en esta versión	Numeral 3.31
No existía en esta versión	Numeral 3.32
No existía en esta versión	Numeral 3.35
No existía en esta versión	Numeral 3.36
IV. DEFINICIÓN DE TERMINOS	IV. DEFINICIÓN DE TERMINOS
Numeral 4.1	Eliminado
Numeral 4.2	Numeral 4.1
Numeral 4.3	Numeral 4.2
Numeral 4.4	Numeral 4.3
Numeral 4.5	Numeral 4.4
Numeral 4.6	Numeral 4.5
Numeral 4.7	Eliminado
Numeral 4.8	Eliminado
Numeral 4.9	Eliminado
Numeral 4.10	Numeral 4.7
Numeral 4.11	Numeral 4.8
Numeral 4.12	Numeral 4.10
Numeral 4.13	Eliminado
Numeral 4.14	Numeral 4.11
Numeral 4.15	Numeral 4.14
Numeral 4.16	Numeral 4.15
Numeral 4.17	Eliminado
Numeral 4.18	Numeral 4.17
Numeral 4.19	Numeral 4.18
Numeral 4.20	Eliminado
Numeral 4.21	Numeral 4.20
Numeral 4.22	Eliminado
Numeral 4.23	Eliminado
Numeral 4.24	Numeral 4.23
Numeral 4.25	Eliminado
Numeral 4.26	Eliminado
Numeral 4.27	Eliminado
Numeral 4.28	Numeral 4.25
Numeral 4.29	Numeral 4.28
Numeral 4.30	Numeral 4.29
Numeral 4.31	Numeral 4.30
Numeral 4.32	Numeral 4.31
Numeral 4.33	Numeral 4.32
Numeral 4.34	Numeral 4.33
Numeral 4.35	Numeral 4.34
Numeral 4.36	Eliminado
Numeral 4.37	Numeral 4.35
No existía en esta versión	Numeral 4.6
No existía en esta versión	Numeral 4.9

No existía en esta versión	Numeral 4.13
No existía en esta versión	Numeral 4.16
No existía en esta versión	Numeral 4.19
No existía en esta versión	Numeral 4.21
No existía en esta versión	Numeral 4.22
No existía en esta versión	Numeral 4.24
No existía en esta versión	Numeral 4.26
No existía en esta versión	Numeral 4.27
No existía en esta versión	Numeral 4.28
No existía en esta versión	Numeral 4.29
V. METODOLOGÍA Y APLICACIÓN DE LA GESTIÓN INTEGRAL DEL RIESGO	V. METODOLOGÍA Y APLICACIÓN DE LA GESTIÓN INTEGRAL DEL RIESGO
Numeral 5.1	Numeral 5.1
Numeral 5.1.1	Numeral 5.1.1
Numeral 5.1.2	Numeral 5.1.2
Numeral 5.1.3	Eliminado
Numeral 5.1.4	Eliminado
Numeral 5.2	Numeral 5.2
Numeral 5.3	Numeral 5.3
Numeral 5.3.1	Numeral 5.3.1
Numeral 5.3.2	Numeral 5.3.2
Numeral 5.4	Numeral 5.4
Numeral 5.5	Numeral 5.5
Numeral 5.5.1	Numeral 5.5.1
Numeral 5.5.2	Numeral 5.5.2
Numeral 5.6	Numeral 5.6
Numeral 5.7	Numeral 5.7
Numeral 5.8	Numeral 5.8
Numeral 5.9	Numeral 5.9
No existía en esta versión	Numeral 5.1.2.1
No existía en esta versión	Numeral 5.1.2.2
No existía en esta versión	Numeral 5.1.2.3
No existía en esta versión	Numeral 5.1.2.4
No existía en esta versión	Numeral 5.1.2.4.1
No existía en esta versión	Numeral 5.1.2.4.2
No existía en esta versión	Numeral 5.1.2.4.3
No existía en esta versión	Numeral 5.1.2.5
No existía en esta versión	Numeral 5.1.2.6
No existía en esta versión	Numeral 5.1.2.7
No existía en esta versión	Numeral 5.1.3
No existía en esta versión	Numeral 5.1.4
No existía en esta versión	Numeral 5.1.5
VI. VIGENCIA	VI. VIGENCIA
VII. APROBACIÓN	VII. APROBACIÓN
VIII. ANEXOS	VIII. ANEXOS

Anexo N° 01 Plan de Gestión Integral del Riesgo	Eliminado
Anexo N° 01 Registro de Análisis del Contexto y Partes Interesadas	Eliminado
Anexo N° 01 Registro para Priorización de Procesos	Eliminado
Anexo N° 01 Registro de Evaluación de Controles Existentes/Implementados	Anexo N° 02 Registro N° 3: Evaluación de Controles Existentes/Implementados
Anexo N° 02 Técnicas Utilizadas en la Gestión del Riesgo	Anexo N° 02 Tabla N° 2: Técnicas Utilizadas en la Gestión del Riesgo
Anexo N° 03 Tablas para la Gestión Integral del Riesgo: Tabla N° 1.1: Tipos de Riesgo	Anexo N° 02 Tabla N° 4: Tipos de Riesgo
Anexo N° 03 Tablas para la Gestión Integral del Riesgo: Tabla N° 1.2: Categoría de Riesgos del Proyecto	Anexo N° 02 Tabla N° 5: Categoría de Riesgos de Proyecto
Anexo N° 03 Tabla N° 02: Fuente del Riesgo	Anexo N° 02 Tabla N° 6: Fuente del Riesgo
Anexo N° 03 Tabla N° 03: Probabilidad	Anexo N° 02 Tabla N° 7: Niveles de Probabilidad
Anexo N° 03 Tabla N° 4.1: Impacto para Riesgos en General	Anexo N° 02 Tabla N° 8: Niveles de Impacto para Riesgos en General
Anexo N° 03 Tabla N° 4.2: Impacto para Riesgos en Seguridad de la Información	Anexo N° 02 Tabla N° 9: Niveles de Impacto para Riesgos en Seguridad de la Información
Anexo N° 03 Tabla N° 4.3: Impacto para Riesgos de Proyectos	Anexo N° 02 Tabla N° 10: Niveles de Impacto para Riesgos en Proyectos
Anexo N° 03 Tabla N° 05: Matriz de Probabilidad de Impacto o Mapa de Calor (Probabilidad x Impacto)	Anexo N° 02 Tabla N° 11: Mapa de Riesgos (Probabilidad x Impacto)
Anexo N° 03 Tabla N° 06: Tipos de Control Existente/Implementado	Anexo N° 02 Tabla N° 12: Tipos de control Existentes/Implementados
Anexo N° 03 Tabla N° 07: Criterios para Análisis del control Existente/Implementado	Anexo N° 02 Tabla N° 13: Criterios para Análisis del control Existente/Implementado
Anexo N° 03 Tabla N° 08: Rangos del Resultado de la Calificación del Control Existente/Implementado	Anexo N° 02 Tabla N° 14: Rangos del Resultado de la Calificación del Control Existente/Implementado
Anexo N° 03 Tabla N° 09: Respuesta al Riesgo	Anexo N° 02 Tabla N° 15: Tipos de respuesta al Riesgo
Anexo N° 03 Tabla N° 10: Criterios para la Respuesta al Riesgo en la Etapa de Tratamiento	Anexo N° 02 Tabla N° 16: Criterios para la Respuesta al Riesgo en la Etapa de Tratamiento
Anexo N° 03 Tabla N° 11: Estado de Avance de Implementación	Anexo N° 02 Tabla N° 17: Estado de Avance de Implementación
Anexo N° 03 Tabla N° 12: Nivel de Efectividad del Control Implementado	Anexo N° 02 Tabla N° 18: Nivel de Efectividad del Control Existente/Implementado
Anexo N° 03 Tabla N° 13: Estado del Riesgo	Anexo N° 02 Tabla N° 19: Estado del Riesgo

Anexo N° 04 Plan de Gestión de Oportunidades	Anexo N° 04 Registro N° 5: Plan de Gestión de Oportunidades
Anexo N° 05 Tablas para la Gestión de Oportunidades - Tabla N° 01: Fuente de Oportunidad	Anexo N° 04 Tabla N° 25: Fuente de Oportunidad
Anexo N° 05 Tablas para la Gestión de Oportunidades - Tabla N° 02: Tipo de Oportunidad	Anexo N° 04 Tabla N° 26: Tipo de Oportunidad
Anexo N° 05 Tablas para la Gestión de Oportunidades - Tabla N° 03: Probabilidad de la Oportunidad	Anexo N° 04 Tabla N° 27: Niveles de Probabilidad de la Oportunidad
Anexo N° 05 Tablas para la Gestión de Oportunidades - Tabla N° 04: Criterios de Evaluación de Oportunidades	Anexo N° 04 Tabla N° 28: Criterios de Evaluación de Impacto de la Oportunidad
No existía en esta versión	Anexo N° 01 Registro N° 1: Reporte de Eventos de Pérdida Registro N° 1.1: Eventos de Pérdida Tabla N° 1: Tipos de Eventos de Pérdida
No existía en esta versión	Anexo N° 02 Registro N° 2: Plan de Acción Anual - Medidas de Control (PAAMC) Tabla N° 3: Preguntas Guía para la Identificación de Riesgos
No existía en esta versión	Anexo N° 03 Tabla N° 20: Situaciones Susceptibles de Riesgos de Corrupción Tabla N° 21: Preguntas Guías para Identificar Riesgos de Corrupción Tabla N° 22: Criterios para Identificar el Riesgo de Corrupción Tabla N° 23: Tipos de Corrupción Registro N° 4: Criterios para evaluar el Impacto en Riesgos de Corrupción Tabla N° 24: Mapa de Riesgos de Corrupción (Probabilidad x Impacto)
No existía en esta versión	Anexo N° 04 Tabla N° 29: Mapa de las Oportunidades Tabla N° 30: Respuesta a las Oportunidades
No existía en esta versión	Anexo N° 05 Registro N° 6: Reporte del Avance de la Gestión del Riesgo y Oportunidades
No existía en esta versión	Anexo N° 06 Cuadro de Control de Cambios