DIRECTIVA

DI-010-OIR/002

GESTIÓN INTEGRAL DEL RIESGO

PRIMERA VERSIÓN

OFICINA DE INTEGRIDAD Y RIESGOS

ÍNDICE

I. OBJETIVO

Establecer lineamientos, asignación de roles y responsabilidades a los órganos y unidades orgánicas en el proceso de planificación, ejecución, seguimiento y mejora de la Gestión Integral del Riesgo en el Registro Nacional de Identificación y Estado Civil – RENIEC.

II. ALCANCE

La presente directiva es administrada por la Oficina de Integridad y Riesgos – OIR, y las disposiciones contenidas en el presente documento son de aplicación y cumplimiento obligatorio para todos los órganos del RENIEC en los diferentes niveles de la Institución.

III. BASE LEGAL

3.1 **Constitución Política del Perú,** del 30 de diciembre de 1993.

3.2 **Ley Nº 26497**, Ley Orgánica del RENIEC, del 12 julio de 1995 y sus modificatorias.

3.3 **Ley Nº 27658**, Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y sus modificatorias.

3.4 **Ley N° 27785**, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, del 23 de Julio 2002 y modificatorias.

3.5 **Ley Nº 28716**, Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.

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

3.7 **Decreto Legislativo N° 1412**, Ley de Gobierno Digital, del 13 de setiembre de 2019.

3.8 **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**.**

3.9 **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.

3.10 **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.

3.11 **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.

3.12 **Decreto Supremo Nº 046-2014-PCM**, aprueba la Política Nacional para la Calidad, del 01 de julio de 2014 y Anexo, del 02 de julio de 2014.

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

3.14 **Decreto Supremo N° 044-2018-PCM**, aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021, del 26 abril de 2018, cuya vigencia ha sido prorrogada hasta la actualización de la Política

Nacional de Integridad y Lucha contra la corrupción, mediante Decreto Supremo N° 180-2021-PCM.

3.15 **Decreto Supremo N° 038-2021-PCM**, aprueba la Política Nacional de Gestión de Riesgos de Desastres al 2050, del 01 de marzo del 2021.

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

3.17 **Decreto Supremo N° 029-2021-PCM,** aprueba el Reglamento del Decreto Legislativo N° 1412 Ley de Gobierno Digital, del 19 de febrero de 2021.

3.18 **Decreto Supremo Nº 103-2022-PCM**, aprueba la Política Nacional de Modernización de la Gestión Pública al 2030, del 21 de agosto de 2022.

3.19 **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.

3.20 **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.

3.21 **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 modificatorias.

3.22 **Resolución de Contraloría Nº 320-2006-CG**, aprueba las Normas de Control Interno, del 03 de noviembre de 2006.

3.23 **Resolución de Contraloría N° 146-2019-CG**, 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 y modificatorias.

3.24 **Resolución Directoral N° 001-2015-INACAL/DN**, aprueba, entre otras, la Norma Técnica Peruana NTP-ISO 9001:2015, Sistema de Gestión de la Calidad – Requisitos. Sexta Edición, del 05 de octubre de 2015.

3.25 **Resolución Directoral N° 012-2017-INACAL/DN**, aprueba 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.

3.26 **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.

3.27 **Resolución Jefatural N° 183-2020/JNAC/RENIEC,** reconforman el Comité de Gobierno Digital del Registro Nacional de Identificación y Estado Civil, del 17 de noviembre de 2020.

3.28 **Resolución Jefatural N° 144-2021/JNAC/RENIEC,** aprueba el Plan Estratégico Institucional 2021-2025 del RENIEC, del 02 de agosto 2021.

3.29 **Resolución Jefatural N° 231-2021/JNAC/RENIEC**, aprueba el Plan de Continuidad Operativa, del 31 de diciembre del 2021.

3.30 **Resolución Jefatural N°000022-2022/JNAC/RENIEC,** deja sin efecto el Artículo Segundo de la Resolución Jefatural N° 183-2020/JNAC/RENIEC (17NOV2020), designa a la Líder de Gobierno y Transformación Digital del Registro Nacional de Identificación y Estado Civil – RENIEC y reconforma el Comité de Gobierno Digital del Registro Nacional de Identificación y Estado Civil – RENIEC, constituido mediante la Resolución Jefatural N° 107-2019/JNAC/RENIEC (22JUL2019) y reconformado por la Resolución Jefatural N° 156- 2019/JNAC/RENIEC (26SET2019) y la Resolución Jefatural N° 183-2020/JNAC/RENIEC (17NOV2020).

3.31 **Resolución Jefatural N° 000086-2021/JNAC/RENIEC,** que aprueba el Reglamento de Organización y Funciones del RENIEC del 04 de mayo de 2021.

3.32 **Resolución Jefatural N° 000162-2022/JNAC/RENIEC,** que aprueba la actualización de la Política y Objetivos de la Gestión Integral del Riesgo, del RENIEC del 26 de setiembre de 2022.

3.33 **Resolución Jefatural N° 000146-2022/JNAC/RENIEC,** que aprueba la Política de Integridad y Lucha contra la corrupción en el RENIEC, del 2 de setiembre de 2022.

3.34 **Resolución Jefatural N° 000141-2022/JNAC/RENIEC,** que aprueba la Política y Objetivos Antisoborno, del 19 de agosto de 2022.

3.35 **Resolución de Secretaría de Integridad Pública N° 001-2019-PCM/SIP,** que aprueba la Directiva N° 002-2021-PCM/SIP “Lineamientos para la implementación de la función de integridad en las entidades de la administración pública”, del 24 de julio del 2019.

3.36 **Resolución de Secretaría de Integridad Pública N° 002-2021-PCM/SIP,** que aprueba la Directiva N° 002-2021-PCM/SIP “Lineamientos para fortalecer una cultura de integridad en las entidades del sector público”, del 28 de junio del 2021.

3.37 **Resolución Secretarial N° 064-2020/SGEN/RENIEC**, aprueba, entre otras, la Directiva DI-445-GTH/014 “Código de Conducta para Servidores Civiles del RENIEC”, del 08 de octubre 2020.

3.38 **Resolución Secretarial Nº 092-2021/SGEN/RENIEC**, aprueba el Mapa de Procesos de nivel 0 y 1 de los procesos transversales del RENIEC, del 09 de diciembre del 2021.

3.39 **Resolución Secretarial Nº 030-2022/SGEN/RENIEC,** aprueba la Directiva DI-001-OPP/001 “Documentos Normativos del RENIEC”, del 17 de abril de 2022.

IV. TÉRMINOS Y DEFINICIONES:

4.1 Amenaza

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

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

Para riesgos de desastres, es la potencial ocurrencia de un evento físico de origen natural o inducido por la acción humana de manera accidental o premeditada, con una severidad tal que pueda causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes e infraestructura.

4.2 Activo de Información

Es todo recurso de información, software, físico o servicio que contenga y/o manipule información del RENIEC.
Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de Información para que las organizaciones funcionen y consigan sus objetivos

4.3 Contexto de la Organización

Es el proceso en el que definen los parámetros internos y externos que se deben considerar cuando se identifica y gestiona el riesgo. factores internos tales como los valores, cultura, conocimiento y desempeño de la entidad, factores externos tales como entornos legales, tecnológicos, de competitividad, de mercados, culturales, sociales y económicos.

4.4 Corrupción

Es 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.

4.5 Dueño del Proceso

Es la persona encargada de facilitar o asegurar la disponibilidad de los recursos para la implementación de la Gestión por Procesos. Asume responsabilidad respecto al desarrollo de las actividades propias del proceso misional, en permanente coordinación y acuerdo con los directores o subdirectores o jefes involucrados en el alcance.

4.6 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. Son designados por el dueño del proceso y funcionarios responsables de los órganos que participan del proceso.

4.7 Evento

Un evento puede ser una fuente de riesgo, pudiendo tener una o más ocurrencias, varias causas y varias consecuencias. ocurrencia o cambio de un conjunto particular de circunstancias.

4.8 Evento de seguridad de la información

Una ocurrencia identificada en el estado de un sistema, servicio, red o cualquier otro activo de seguridad de la información; indicando una posible violación a la política de seguridad de la información, falla en los controles o

una situación previamente desconocida que puede ser relevante para la Seguridad de la Información.

4.9 Fuente de Riesgo

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

4.10 Gestión Integral del Riesgo (GIR)

Es la aplicación sistemática de políticas, procedimientos y prácticas de gestión con la finalidad de brindar 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, 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.

4.11 Gestor Líder de Riesgos

Responsable designado por el órgano o dueño del proceso, quien realizará las coordinaciones con los órganos de asesoramiento técnico encargados de la gestión integral del riesgo.

4.12 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.

4.13 Impacto o Consecuencias

Resultado de un evento o incidente que afecta a los objetivos de la entidad. El impacto puede ser positivo (oportunidad) o negativo con relación a las consecuencias que puede ocasionar a la entidad la materialización del riesgo. En el caso de los riesgos de Seguridad de la Información es el daño sobre el activo derivado de la materialización de la amenaza.

4.14 Incidente de Seguridad de Información

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

La clasificación del incidente es de dos tipos:

- Incidente de Seguridad Digital: Se ven comprometidos los activos digitales (sistemas, archivos, hardware, personas, etc.) cuya información es provista hacia los grupos de interés (información dirigida al ciberespacio).

- Incidente de Seguridad de la Información: Información en general que es provista en el marco del SGSI – eventos de seguridad de la información.

4.15 Medida de Control

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

4.16 Plan de Acción Anual – Medidas de Control (PAAMC)

Documento donde se registran las acciones para gestionar los riesgos identificados en los procesos de la entidad.

4.17 Plan de Contingencia

Documento que contiene las acciones de ejecución inmediata en respuesta al riesgo materializado.

4.18 Política de la Gestión Integral del Riesgo

Es la declaración y compromiso de la Alta Dirección respecto a la gestión integral del riesgo en la entidad, establece 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 (RENIEC), es aprobada por la Jefatura Nacional.

4.19 Probabilidad

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

4.20 Producto

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

4.21 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.

4.22 Proceso Gestión Integral del Riesgo

Comprende la realización de actividades necesarias para dirigir y controlar 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.

4.23 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. (NTP ISO 31000:2018).

4.24 Riesgo de corrupción

Posibilidad de que ocurra una conducta, por acción u omisión que refleje el mal uso de la función o el poder público, la obtención de un beneficio indebido para sí o para terceros y que constituya un delito contra la administración pública.

Si se materializa un riesgo de corrupción, se afecta la confianza de la ciudadanía en la entidad, así como el correcto y regular funcionamiento de la administración pública.

4.25 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 proceso.

4.26 Tolerancia al Riesgo

Es la capacidad de aceptar el riesgo, según el nivel que la Entidad puede o está dispuesta a soportar, con el fin de lograr sus objetivos.

V. RESPONSABILIDADES

5.1 Los órganos y unidades orgánicas del RENIEC son responsables de cumplir lo normado en la presente Directiva; así como de establecer acciones para asegurar la implementación progresiva de la Gestión Integral del Riesgo en los procesos a su cargo y en los que participa.

5.2 Es responsabilidad de la Oficina de Planificación y Presupuesto (OPP), proponer ante la Gerencia General (GG) y Secretaría General (SGEN) a los dueños de los procesos estratégicos, de soporte y misionales del RENIEC. Quienes son responsables a su vez de establecer las acciones para gestionar los riesgos, que de materializarse pueden impedir el logro de los objetivos de sus procesos.

5.3 La OPP formula el diagnóstico situacional respecto al diseño y funcionamiento de sus procesos operativos que permiten la producción y entrega de productos y servicios a la población (contexto interno), así como evaluar lo relacionado de escenarios contextuales a nivel nacional (contexto externo); procesos que servirán como insumo para la identificación de riesgos y oportunidades en los procesos de la entidad, para ello coordinará con la OIR.

5.4 Es responsabilidad de la OIR coordinar con la Oficina de Formación Ciudadana e Identidad (OFCI) y Oficina de Potencial Humano (OPH), la elaboración del plan anual de capacitación de la Gestión Integral del Riesgo, y con la Oficina de Comunicaciones y Prensa (OCP), la elaboración del Plan Anual de Sensibilización.

5.5 Es responsabilidad de la OIR coordinar con los órganos y unidades orgánicas de la entidad los aspectos técnicos relevantes de la Gestión Integral del Riesgo según su competencia (seguridad de la información, continuidad operativa, proyectos, y desastres).

5.6 La OIR es responsable de administrar, proponer, actualizar y realizar el seguimiento del cumplimiento del marco normativo de la Gestión Integral del Riesgo.

5.7 La OIR es responsable de realizar el seguimiento y evaluación del reporte de avance del Plan de Acción Anual Medidas de Control (PAAMC), y plan de

gestión de oportunidades (PGO), remitido por los órganos designados como dueños de proceso.

5.8 Es responsabilidad de la OIR reportar a la Alta Dirección el estado de evaluación de los riesgos identificados en los procesos, así como el resultado del seguimiento en la implementación de las medidas de control del PAAMC.

5.9 La Oficina de Seguridad y Defensa Nacional (OSDN) coordina con la OIR la gestión de los riesgos de seguridad física y gestión de riesgo de desastres, durante el proceso de implementación, ejecución y sostenibilidad de la Gestión Integral del Riesgo.

5.10 La OPP, según sus competencias realizara una propuesta de productos priorizados de la entidad que será remitida a la SGEN para su evaluación y de ser viable, se concrete en la propuesta de los productos priorizados que van a ser incorporados en el Plan de Acción Anual Medidas de Control (PAAMC).

5.11 La OCP es responsable de elaborar y ejecutar en coordinación con la OIR el plan de sensibilización de la Gestión Integral del Riesgo comunicando los resultados.

5.12 Es responsabilidad de la Oficina de Tecnologías de la Información (OTI) el mantener permanentemente identificados y actualizados los riesgos relacionados a la seguridad de la información, tanto en su definición, implementación y control, estableciendo políticas y procedimientos basados en buenas prácticas, según la normativa nacional e internacional, debiendo reportar a la OIR para las acciones correspondientes.

5.13 La OPH es responsable de velar por que los procesos de incorporación, compensaciones, evaluación de rendimiento, capacitación, seguridad y salud en el trabajo, relaciones laborales y aplicación de medidas disciplinarias se desarrollen sobre los principios de equidad, objetividad e imparcialidad, considerando la segregación de funciones que permita minimizar la exposición a los riesgos operativos y/o de corrupción.

5.14 La Secretaria General (SGEN) y la Gerencia General son responsables de supervisar que la Gestión Integral del Riesgo se incorpore progresivamente en los procesos de la Entidad, que están a su cargo.

5.15 Es responsabilidad de la SGEN presentar la propuesta de productos priorizados elaborada por la Oficina de Planificación y Presupuesto (OPP) a la Jefatura Nacional (JNAC) para su aprobación.

5.16 La SGEN es responsable del visado del PAAMC y presentar a la JNAC para su aprobación y posterior remisión mediante el aplicativo informático a la CGR.

5.17 Es responsabilidad de la SGEN y de la Gerencia General, disponer a los órganos y unidades orgánicas bajo su competencia la implementación de las medidas de control propuestas para el tratamiento de los riesgos identificados en los productos priorizados y no priorizados.

VI. DISPOSICIONES GENERALES

6.1 Los órganos y unidades orgánicas designan y/o ratifican a los Gestores Líderes y equipos de riesgos; reportan a la OIR cuando se produzca algún cambio.

6.2 Los órganos designados como dueños del proceso, en coordinación con los órganos que participan en el mismo, formulan y/o actualizan su Plan de Acción Anual Medidas de Control (PAAMC). En caso se requiera, solicitan asistencia técnica a la OIR.

6.3 Los órganos y unidades orgánicas que participan en el proceso deben mantener un registro de incidentes y/o eventos que se detecten en los procesos a su cargo, de modo que este sirva como un insumo de información para la gestión de riesgos en sus procesos.

6.4 La OIR brinda asesoría y asistencia técnica a los órganos y unidades orgánicas en el marco del proceso de implementación de la gestión integral del riesgo en los procesos de la entidad.

6.5 Los órganos designados como dueños de proceso usan como insumo la evaluación del contexto interno/externo realizada por la OPP, con base a los cambios que se produzcan y los recursos disponibles, a fin de identificar, analizar, valorar y tratar los riesgos; estableciendo medidas de control orientadas a reducir las causas del riesgo de manera eficaz, oportuna y eficiente, con la finalidad de mitigar los efectos o consecuencias de la materialización de los riesgos y puedan ser implementadas por la entidad al 31 diciembre de cada año. Dejando constancia de las reuniones de trabajo sostenidas en las actas suscritas.

6.6 Los órganos que participan en los procesos establecidos por la entidad deben reportar a los dueños del proceso los avances en la implementación de sus medidas de control dos (02) días hábiles siguientes culminado el mes de evaluación, a fin de crear el tiempo suficiente para permitir al dueño del proceso, valide y evalúe previamente el reporte mensual que realiza a la OIR.

6.7 Los órganos designados como dueños del proceso reportaran sus Planes de Gestión Integral del Riesgo de acuerdo con el siguiente detalle:

a. Plan de Acción Anual Medidas de control (PAAMC) de productos priorizados, reportan mensualmente a la OIR dentro de los **5 días hábiles** siguientes culminado el mes en evaluación, las evidencias de las acciones específicas que permitirán implementar las medidas de control (MC), al correo institucional Implementación del Sistema de Control Interno (implementacionSCI@reniec.gob.pe), y mediante el Sistema Integrado de Tramite Documentario-SITD el reporte semestral y anual, indicando el enlace (link) de la carpeta compartida que contiene las evidencias.

b. Plan de Acción Anual Medidas de Control (PAAMC) de productos no priorizados, reportan trimestralmente a la OIR dentro de los **5 días hábiles** siguientes culminado el mes en evaluación, las evidencias de las acciones específicas que permitirán implementar las medidas de control (MC), mediante el Sistema Integrado de Tramite Documentario-SITD, indicando el enlace (link) de la carpeta compartida que contiene las evidencias.

6.8 En caso se presente la necesidad de reformular y/o ampliar los plazos para la implementación de las medidas de control o acciones propuestas en el Plan de Acción Anual Medidas de control (PAAMC), los órganos designados como dueños de los procesos deberán solicitar la reformulación o ampliación, justificando el motivo de la modificación a la Oficina de Integridad y Riesgos para su evaluación y recomendaciones, esta reportara a la Alta Dirección para su aprobación.

6.9 El Plan de Acción Anual Medidas de Control (PAAMC), debe ser aprobado por el dueño del proceso y comunicado a los órganos que participan en el proceso.

6.10 La OIR coordinará con la SGEN la formulación, aprobación, y el seguimiento en la ejecución del Plan de Acción Anual Medidas de Control (PAAMC).

6.11 La OIR juntamente con los órganos y unidades orgánicas de la entidad formularan las propuestas técnicas orientadas a la consolidación, mejoramiento y sostenibilidad de la Gestión Integral del Riesgo.

VII. DISPOSICIONES ESPECÍFICAS

7.1 PLANIFICACIÓN DE LA GESTIÓN DEL RIESGO

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.

La OIR planifica anualmente y de forma oportuna, las actividades que implican la gestión de riesgos con los recursos necesarios, priorizando los procesos misionales y críticos.

7.2 IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden impedir o contribuir (oportunidades) el logro de objetivos en la entidad, para ello es importante contar con información apropiada y actualizada.

En el caso de la identificación de riesgos de seguridad de información se debe realizar previamente el inventario de activos de información con su respectiva valorización (confidencialidad, integridad y disponibilidad)

En la identificación del riesgo, se debe tener en cuenta los factores, situaciones o eventos que podrían afectar el cumplimiento de los objetivos del proceso y del producto, tales como:

a. Identificar factores que puedan afectar los plazos y estándares de calidad establecidos en los productos a ser brindados a los ciudadanos.

b. El análisis de sus operaciones, procesos, actividades y tareas.

c. Las amenazas y las oportunidades.

d. Las vulnerabilidades y las capacidades.

e. Comportamiento y capacidades humanas, la organización del trabajo y otros factores humanos.

f. La infraestructura, servicios de apoyo y equipamiento.

g. Las normas legales, internas y otros suscritos por la Entidad.

h. La gestión de proveedores y subcontratación de actividades, productos y/o servicios, susceptibles de generar riesgos.

i. Propuestas de modificación organizacional, nuevos procesos y/o mejora de procesos.

j. Análisis de sus procesos y productos que tengan mayor exposición 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).

k. Fuga de información el cual podría dañar la imagen del RENIEC.

l. Analizar si los riesgos identificados:

- ✓ Podrían generar actos de corrupción (soborno) u otras clases de riesgo de conducta irregular
- ✓ Podrían generar fraudes financieros o contables (registros contables y administrativos falsos), sobrecostos o transferencia de recursos para fines distintos al original.
- ✓ Podrían afectar el cumplimiento de las funciones desarrolladas por los funcionarios y servidores al encontrarse influenciados, inducidos o presionados a efectuar conductas irregulares.
- ✓ Podrían generar posible influencia de consultores o actores externos en las decisiones de los funcionarios para realizar requerimientos de bienes o servicios.
- ✓ Podrían generar pagos tardíos (retrasados) a los proveedores.
- ✓ Podrían generar el favorecimiento a un postor o postulante, dentro de un proceso de contratación.

7.3 ANÁLISIS DEL RIESGO

El análisis consiste en determinar la probabilidad por el impacto o consecuencias; de acuerdo al siguiente detalle:

a. **La probabilidad** de que suceda un determinado evento, el cual puede medirse en términos de frecuencia (eventos ocurridos en un determinado periodo de tiempo, revisar el registro de incidentes) o factibilidad (presencia de factores externos – internos que pueden propiciar el riesgo).

b. **El impacto** puede ser positivo (oportunidad) al logro de objetivos o negativo con las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

7.4 VALORACIÓN DEL RIESGO

La valoración del riesgo implica comparar los resultados del análisis del riesgo (probabilidad e impacto), para estimar el nivel de exposición inicial del riesgo (Riesgo inherente) y confrontar frente a los controles existentes, con el fin de establecer el nivel de exposición del riesgo final (riesgo residual), el resultado se analiza con el criterio de aceptación de la entidad, estableciendo 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 y determinación de las “medidas de control”, con la finalidad de mitigar el riesgo.

7.5 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo tiene como objetivo diseñar, evaluar, seleccionar e implementar medidas de control para modificar el nivel de exposición de los riesgos identificados en los procesos, proporcionar nuevos controles o modificar los existentes.

En los planes de tratamiento del riesgo se plasman las acciones de respuesta ante los riesgos que afectan negativamente o contribuyen

(oportunidades), al logro de los objetivos institucionales por causas que tienen origen en procesos, tecnología, eventos externos o errores de personas.

Para los planes de tratamiento de riesgos de seguridad de información se debe considerar la implementación de controles que son descritos en la NTP-ISO/IEC 27002 con la finalidad efectuar las estrategias de respuesta, en el caso de los riesgos negativos (eliminar, reducir, transferir, aceptar); y para el caso de los riesgos positivos (explotar, compartir, mejorar, aceptar).

En el caso de los planes de tratamiento de riesgos de corrupción se proponen las acciones de respuesta ante riesgos que afectan negativamente la reputación de la entidad, por causas relacionadas por acciones u omisiones de servidores con el propósito de obtener para si o para terceros, un beneficio indebido de carácter económico o no económico u otras ventajas, utilizando indebidamente su posición en el RENIEC.

En el tratamiento de los riesgos de corrupción la tolerancia es cero, es decir se deben tomar acciones de respuesta inmediata independiente del nivel de exposición del riesgo.

Los Gestores Líderes de Riesgos y sus equipos de trabajo de los procesos que han sido designados por los dueños de los procesos, deben coordinar con los órganos que participan en el proceso y con los órganos de apoyo involucrados en la elaboración de los planes de tratamiento, estos deben contener las medidas de control, orientadas a reducir las causas del riesgo de manera eficaz, oportuna y eficiente con la finalidad de mitigar los efectos o consecuencias de la materialización de los riesgos.

7.5.1 Criterios de prioridad para el Tratamiento del Riesgo:

Los planes de tratamiento de riesgos de acuerdo con su nivel de exposición tienen los siguientes criterios de prioridad para su implementación:

Nivel de exposición	Nivel de Prioridad
Muy alto	1º
Alto	2º
Medio	3º

Elaboración OIR

7.6 SEGUIMIENTO Y REVISIÓN

Esta etapa es realizada por el dueño del proceso y consiste en verificar si la implementación de las medidas de control establecidas para el tratamiento de riesgos contenidos en el **Plan de Acción Anual – Medidas de Control (PAAMC) o Plan de Gestión Integral del Riesgo** de los productos (priorizados y no priorizados) se están implementando de acuerdo con lo planificado. Asimismo, evalúa el cumplimiento y la eficacia en la implementación de las medidas de control o tratamiento del riesgo.

La OIR solicitará periódicamente el reporte de avance en la implementación de las medidas de control, estos avances deben ser acreditados con documentación que evidencie la implementación.

- 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 continuo por parte del dueño del proceso para asegurar que circunstancias cambiantes no alteren los objetivos del proceso o producto.

7.7 COMUNICACIÓN Y CONSULTA

El propósito de la comunicación y consulta es asistir a las partes interesadas 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.

a. 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.

b. El RENIEC 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 a través de la directiva correspondiente.

7.8 REGISTRO E INFORME

Los resultados de la Gestión Integral del Riesgo se deben documentar, aprobar e informar a través de los mecanismos establecidos en el “Manual de Gestión Integral del Riesgo”.

El Dueño del Proceso es responsable de la elaboración, registro, actualización, disposición y custodia de la información, el cual debe ser reportado a la Oficina de Integridad y Riesgos conforme a lo indicado en el “Manual de Gestión Integral del Riesgo”.

VIII. VIGENCIA

Entrará en vigencia a partir de su aprobación.

IX. APROBACIÓN

Será aprobada mediante Resolución Secretarial.