INSTRUCTIVO DE LA HERRAMIENTA DE GESTIÓN INTEGRAL DE RIESGOS Y GESTIÓN DE OPORTUNIDADES 2023

Oficina de Integridad y Riesgos

GESTIÓN INTEGRAL DE RIESGOS

- La gestión integral de riesgos es un proceso que permite identificar, analizar, evaluar los riesgos, así como determinar e implementar medidas de control para mitigar los riesgos que pueden afectar el logro de los objetivos del RENIEC y que afecta a la entrega de bienes y servicios a la Ciudadanía.
- La base para la metodología está en la Directiva vigente de la Contraloría General de la República (CGR) para la implementación del Sistema de Control Interno (SCI), Directiva N° 006-2019-CG/INTEG, Implementación del Sistema de Control Interno en las entidades del Estado y sus modificatorias.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

CONCEPTOS

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."

Riesgo:
Es la posibilidad de ocurrencia de un evento adverso, respecto al cumplimiento de los objetivos estratégicos institucionales. Efecto de la incertidumbre sobre la consecución de los objetivos.

Causa:
Motivo o razón por la que el riesgo ocurre y es de impacto negativo para la entidad.

Efecto:
Resultado de un evento o incidente que afecta a los objetivos de la entidad. La materialización del riesgo, es de impacto negativo para la entidad. En el caso de los riesgos de Seguridad de la Información es el daño sobre el activo derivado de la materialización de la amenaza.

Oportunidad:

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

Evento positivo:

Motivo o razón para que la oportunidad se de y es de impacto positivo para la entidad.

Beneficio:

Resultado de un evento o incidente que afecta a los objetivos de la entidad.
El impacto es positivo (oportunidad)

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

CONCEPTOS

Medida de Control (Control)

"*Las políticas, procedimientos, técnicas y otros mecanismos que permitan reducir de manera eficaz, oportuna y eficiente los riesgos.*"

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."

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."

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

CONCEPTOS

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.”

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.”

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

CONCEPTOS

Producto priorizado:

“Es el producto incorporado a la gestión de riesgos para identificar por primera vez lo riesgos que pudieran afectar las condiciones y cualidades con las que debe ser brindado, a fin de determinar medidas de control que pudieran reducirlos.”

Producto revaluado:

“Es el producto incorporado a la gestión de riesgos sobre el cual se revalúan los riesgos identificados en años anteriores para determinar si alcanzaron niveles de tolerancia aceptables por la entidad y para identificar nuevos riesgos que pudieran afectar las condiciones y cualidades con las que se brinda.”

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

TIPOS DE RIESGOS

• Riesgo de desempeño: Posibilidad de que el producto no se entregue a los usuarios finales con sus atributos esperados, lo cual afecte el logro de los resultados u objetivos institucionales.
• Riesgo que afecta la integridad pública: Posibilidad de que una determinada conducta transgreda, por acción u omisión, el respeto de los valores de la organización, así como de los principios, deberes y normas relacionadas al ejercicio de la función pública y configure una práctica contraria a la ética o práctica corrupta.

Riesgo de Desempeño - Operativo: Posibilidad de ocurrencia de efectos adversos debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos.
Riesgos de Desempeño - Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Riesgos de Desempeño - Desastres: Posibilidad de ocurrencia de 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).
Riesgo que afecta a la Integridad Pública - Corrupción: Posibilidad de que ocurra un comportamiento, por acción u omisión, derivado del mal uso de la función o poder público, para obtener o perseguir la obtención de una ventaja o beneficio irregular, lo cual configura un delito.
Riesgo que afecta a la Integridad Pública - Inconducta Funcional: Posibilidad de que ocurra un comportamiento, por acción u omisión, que implica el incumplimiento de funciones y que contraviene el ordenamiento jurídico administrativo y las normas internas de la entidad.
Riesgos Estratégicos: Se asocian con la gobernanza de la entidad. La gestión del riesgo estratégico se enfoca en asuntos globales relacionados con la visión-misión y el cumplimiento de los objetivos institucionales, la clara definición de políticas, el diseño y conceptualización de la entidad por parte de la Alta Dirección.

PREGUNTAS FRECUENTES

MODELO DE GESTIÓN INTEGRAL DE RIESGOS RENIEC

Gestión del Riesgo	Gestión del Plan de Gestión Integral del Riesgo
• Identificación • Análisis • Valoración • Tratamiento	• Planificación • Comunicación y consulta • Registro e Informe
Seguimiento y Revisión	

¿QUÉ ES UN RIESGO?

Es la posibilidad de ocurrencia de un evento adverso o positivo, respecto al cumplimiento de los objetivos estratégicos institucionales.
Efecto de la incertidmbre sobre la consecución de los objetivos. (NTP ISO 31000:018).

¿QUÉ ES LA GESTIÓN DE RIESGOS?

Es un proceso que permite identificar y evaluar los riesgos que pueden afectar el logro de los objetivos de las entidades públicas, relacionados a la provisión de bienes y servicios públicos a la población, así como determinar e implementar medidas para mitigar esos riesgos.

¿QUÉ ES LA GESTIÓN INTEGRAL DEL RIESGO?

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.

¿CUÁL ES LA NORMATIVA?

- Directiva N.°006-2019-CG/INTEG, Implementación del Sistema de Control Interno en las entidades del Estado y sus modificatorias.
- NTP-ISO 31000:2018 Norma Técnica Peruana. Gestión del Riesgo y Directrices.

¿POR QUÉ ES IMPORTANTE?

- Permite mitigar los riesgos que podrían afectar el logro de los objetivos institucionales y la entrega de bienes o provisión de servicios a la población.
- Promueve el aprendizaje y mejora continua de la gestión pública, al generar información valiosa sobre el funcionamiento de la entidad y sobre las estrategias para mitigar los riesgos.
- Fomenta una cultura de prevención en las entidades.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

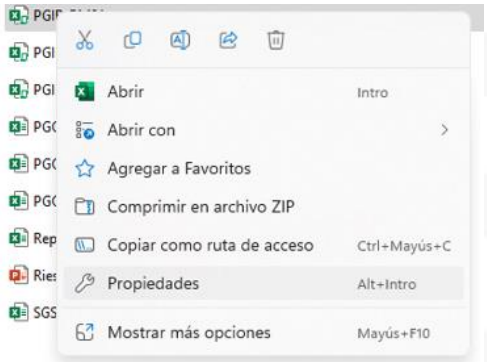
MODELO DE GESTIÓN INTEGRAL DE RIESGOS RENIEC

ETAPAS DE LA METODOLOGÍA

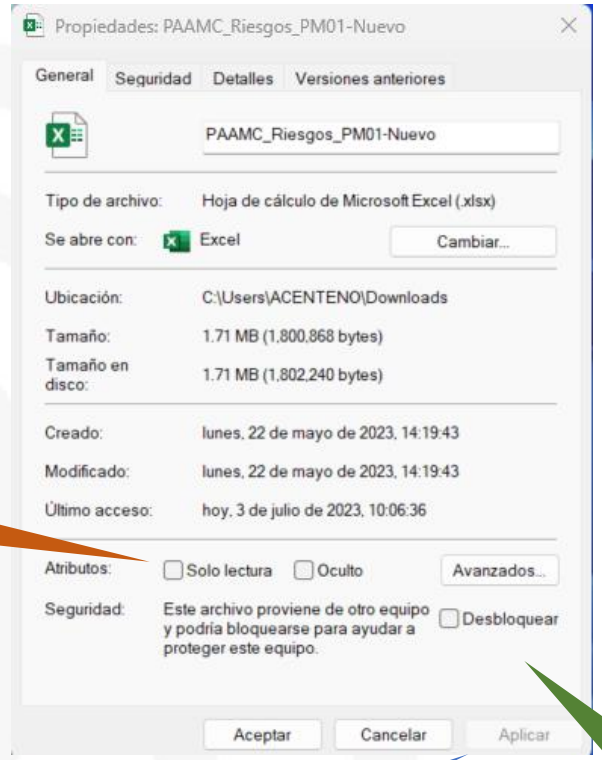
RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PASOS PARA HABILITAR MACRO DE LA HERRAMIENTA GIR

1. Clic derecho en el archivo, e ir a Propiedades



2. En Propiedades:



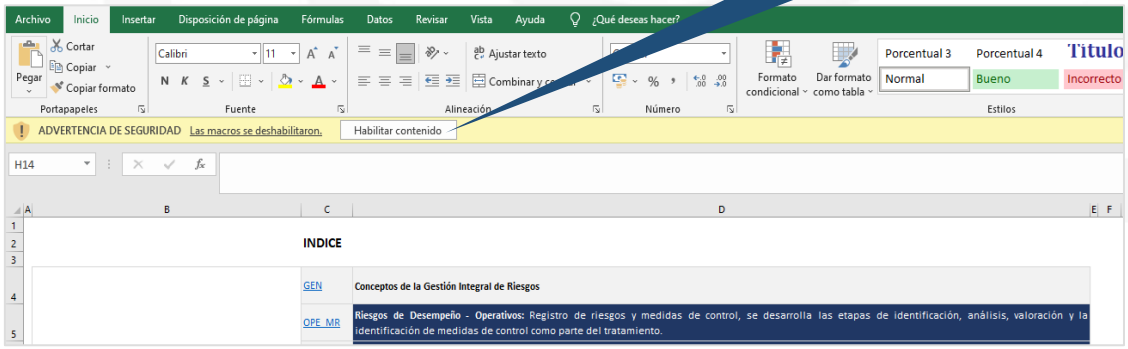
Desmarcar "Solo lectura"

Dar clic en aplicar y aceptar

Dar check "Desbloquear"

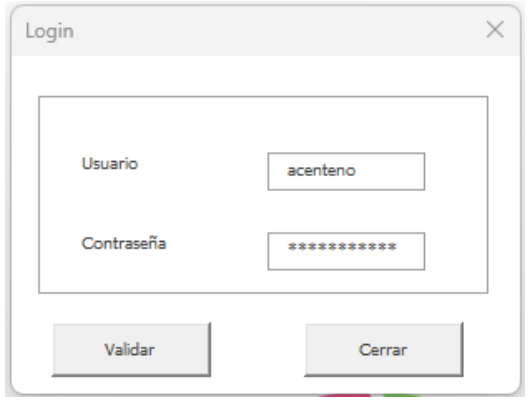
3. Al abrir archivo

Dar clic en "Habilitar macro"



4. Login:

En el campo de texto usuario colocar el usuario de correo electrónico institucional y en el campo contraseña, colocar la clave registrada en el formulario Google enviado por la OIR.



RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

- Es el proceso para establecer los objetivos e implementar todas las actividades de la Gestión Integral del Riesgo, siendo importante una planificación cuidadosa y explicita 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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

HERRAMIENTA DE GESTIÓN INTEGRAL DE RIESGOS

- Está conformado por registros, hojas informativas y un reporte.

Herramienta	Identificación	Análisis	Valoración	Tratamiento	Seguimiento	Revisión
PGIR	✓	✓	✓	✓	✓	✓
PGO	✓	✓		✓	✓	✓

- Cada herramienta, es un archivo en Excel y está compuesto por hojas clasificadas en registros, descripciones y reportes.

Registros	• Hoja en el que se graba información que servirá para la identificación, análisis y tratamiento de riesgos y oportunidades.
Descripciones	• Hoja en la que se brinda descripciones de los valores en lista que se encuentra en los registros, material de apoyo para seleccionar una opción.
Reportes	• Hoja en el que se muestra resumen de resultados, está con fórmulas y no se debe editar, solo visualizar la información. Es útil para la toma de decisiones.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PLAN DE GESTIÓN INTEGRAL DE RIESGOS - PGIR

- Está conformado por registros, hojas informativas y reportes.

GEN	**Conceptos de la Gestión Integral de Riesgos**
OPE_MR	**Riesgos de Desempeño - Operativos:** Registro de riesgos y medidas de control, se desarrolla las etapas de identificación, análisis, valoración y la identificación de medidas de control como parte del tratamiento.
OPE_MC	**Riesgos de Desempeño - Operativos:** Registro de las medidas de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación.
OPE_AC	**Riesgos de Desempeño - Operativos:** Registro de las acciones por cada medida de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación. Asimismo, se registra un comentario por cada mes como resultado del seguimiento del órgano y del oficial de Calidad.
OPE_RE	**Resumen de Desempeño - Operativos:** Muestra descripciones de los valores a usar en la matriz de riesgos y tratamiento.
SIN_MR	**Riesgos de Desempeño - Seguridad de la Información:** Registro de riesgos y medidas de control, se desarrolla las etapas de identificación, análisis, valoración y la identificación de medidas de control como parte del tratamiento.
SIN_MC	**Riesgos de Desempeño - Seguridad de la Información:** Registro de las medidas de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación.
SIN_AC	**Riesgos de Desempeño - Seguridad de la Información:** Registro de las acciones por cada medida de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación. Asimismo, se registra un comentario por cada mes como resultado del seguimiento del órgano y del oficial de Seguridad Digital.
SIN_RE	**Resumen de Desempeño - Seguridad de la Información:** Muestra descripciones de los valores a usar en la matriz de riesgos y tratamiento.
DES_MR	**Riesgos de Desempeño - Desastres:** Registro de riesgos y medidas de control, se desarrolla las etapas de identificación, análisis, valoración y la identificación de medidas de control como parte del tratamiento.
DES_MC	**Riesgos de Desempeño - Desastres:** Registro de las medidas de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación.
DES_AC	**Riesgos de Desempeño - Desastres:** Registro de las acciones por cada medida de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación. Asimismo, se registra un comentario por cada mes como resultado del seguimiento del órgano y del oficial de Calidad.
DES_RE	**Resumen de Desempeño - Desastres:** Muestra descripciones de los valores a usar en la matriz de riesgos y tratamiento.
IN_MR	**Riesgos que afecta la Integridad Pública:** Corrupción e Inconducta Funcional. Registro de riesgos y medidas de control, se desarrolla las etapas de identificación, análisis, valoración y la identificación de medidas de control como parte del tratamiento.
INT_MC	**Riesgos que afecta la Integridad Pública:** Registro de las medidas de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación.
INT_AC	**Riesgos que afecta la Integridad Pública:** Registro de las acciones por cada medida de control, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación. Asimismo, se registra un comentario por cada mes como resultado del seguimiento del órgano y del responsable de función de cumplimiento.
INT_RE	**Resumen de riesgos que afecta la Integridad Pública:** Muestra descripciones de los valores a usar en la matriz de riesgos y tratamiento.

LEYENDA

Aplica para todos los campos con estos colores

	Seleccionar valor de la lista.
	No ingresar data, campo con fórmula.
	Registrar datos en el campo.

MEJ	Registro de problemática y recomendaciones de mejora por producto
CON	Descripciones de las características de cada criterio de evaluación de control. Material de apoyo para evaluar el control propuesto.
NEX	Muestra las combinaciones de nivel de exposición y como se ve afectado por la efectividad del control.
REP	Contiene un resumen de la cantidad de riesgos identificados clasificados por tipo y sub tipo de riesgos, nivel de riesgo inherente, residual, estado de implementación y nivel de efectividad de los mismos. Asimismo, contiene gráficos comparando el nivel de riesgos inherentes y residual.
MRI	Mapa de riesgos antes y después de tratamiento por cada tipo de riesgo, muestra las cantidades en cada cuadrante del mapa de riesgos.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PLAN DE GESTIÓN DE OPORTUNIDADES - PGO

- Está conformado por registros, hojas informativas y un reporte.

Matriz_Oportunidades	•Registro de oportunidades, en el cual se puede identificar y analizar oportunidades.
Acciones_Seguimiento	•Registro de las acciones por cada oportunidad, identificando órgano responsable, fecha de inicio, fin de implementación, medios de verificación. Asimismo, se registra un comentario por cada mes como resultado del seguimiento del órgano y de la OIR.
Descripción	• Descripciones de los niveles de probabilidad, impacto y opciones de tratamiento.
Mapa de Oportunidades	•Contiene el mapa de oportunidades antes y después de tratamiento, muestra las cantidades en cada cuadrante del mapa de oportunidades.

LEYENDA

Aplica para todos los campos con estos colores

	Seleccionar valor de la lista.
	No ingresar data, campo con fórmula.
	Registrar datos en el campo.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identificación de Riesgos

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

IDENTIFICACIÓN DE RIESGOS

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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DE QUÉ PROCESO ESTOY GESTIONANDO EL RIESGO?

PASO 0

En todas las hojas de registro de la herramienta se cuenta con la siguiente cabecera.

VERSIÓN	1	2.0	FECHA DE APROBACIÓN	2	15/06/2023
PROCESO	3	PM01_PROCESO DE LA IDENTIFICACION	TIPO DE PROCESO	4	MISIONAL
ÓRGANO DUEÑO DEL PROCESO	5	Dirección de Registro de Identificación	ÓRGANOS QUE PARTICIPAN EN EL PROCESO	6	DRI, DRIAS, DSR

LEYENDA

1. Versión: Colocar el número de versión.
2. Fecha de aprobación: Registrar la fecha de aprobación por el Dueño de Proceso en formato dd/mm/aaaa.
3. Proceso: Seleccionar el proceso del cual se va a gestionar riesgos.
4. Tipo de Proceso: Campo con fórmula, No editar, al seleccionar el proceso, se visualizará si es misional, soporte o estratégico.
5. Órgano Dueño del Proceso: Seleccionar el órgano que dirige el dueño del proceso.
6. Órganos que participan en el proceso: Registrar los órganos que participan en el proceso, incluyendo al órgano del dueño de proceso, en siglas.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RIESGOS IDENTIFICADOS?

OPERATIVO

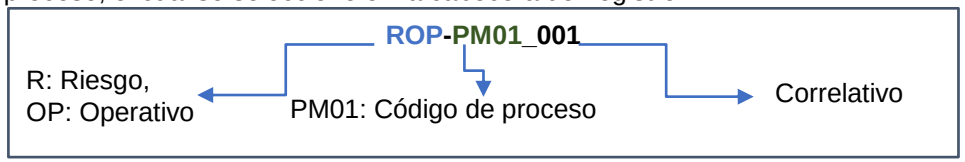
PASO 1

En la hoja *"OPE_MR"*, en la sección *"Identificación"*, registrar los riesgos identificados según la siguiente descripción:

	DATOS GENERALES			IDENTIFICACIÓN			
CODIGO DEL RIESGO	ORIGEN	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)	CAUSA	RIESGO	EFECTO	DESCRIPCIÓN DEL RIESGO
R 1 I_001	2	3	4	5	6	7	8

LEYENDA

1. Código generado automáticamente, tomando como referencia el código del proceso, el cual se selecciono en la cabecera del registro.



2. Lista con opciones de origen (Contexto, Partes interesadas, provisión de productos y servicios y comunicación interna).
3. Producto (Nombre de producto de acuerdo a la definición de Gestión por Procesos, seleccionar el valor de la lista).
4. Producto (Nombre de productos priorizados informados a Contraloría, seleccionar el que corresponda de la lista.

LEYENDA

5. Breve descripción de la causa del riesgo.
6. Breve descripción del riesgo
7. Breve descripción del efecto del riesgo.
8. Descripción del riesgo, considerando, causa y efecto.

EJEMPLO

Debido a errores del personal en el procedimiento de despacho del DNI/DNIe cuando realicen el lotizado del DNI, *podría* ocurrir el extravío y/o perdida del DNIe, ocasionando el incumplimiento de plazos de entrega del DNI/DNIe, generando insatisfacción del ciudadano.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RIESGOS IDENTIFICADOS?

SEGURIDAD DE LA INFORMACIÓN

PASO 1

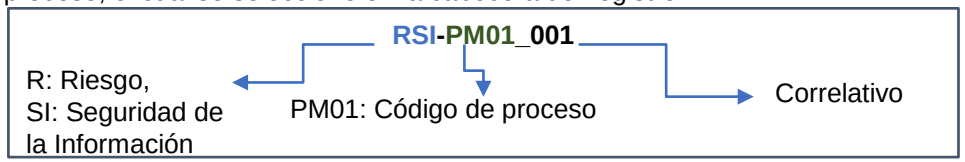
En la hoja *"SIN_MR"*, en la sección *"Identificación"*, registrar los riesgos identificados según la siguiente descripción:

	DATOS GENERALES		
CODIGO DEL RIESGO	ORIGEN	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)
R 1 I_001	2	3	4

IDENTIFICACIÓN				
ACTIVO	AMENAZA	VULNERABILIDAD	EFECTO	DESCRIPCIÓN DEL RIESGO
5	6	7	8	9

LEYENDA

1. Código generado automáticamente, tomando como referencia el código del proceso, el cual se selecciono en la cabecera del registro.



2. Lista con opciones de origen (Contexto, Partes interesadas, provisión de productos y servicios y comunicación interna).
3. Producto (Nombre de producto de acuerdo a la definición de Gestión por Procesos, seleccionar el valor de la lista).
4. Producto (Nombre de productos priorizados informados a Contraloría, seleccionar el que corresponda de la lista.

LEYENDA

5. Nombre del activo identificado
6. Describir brevemente la amenaza
7. Describir brevemente la vulnerabilidad.
8. Describir el efecto, relacionándolo a los pilares de Seguridad de la información, confidencialidad, integridad y disponibilidad.
9. Describir el riesgo considerando activo, amenaza, vulnerabilidad y efecto.

EJEMPLO

Ataques de códigos POR Falta del Proceso de Gestión de Parches maliciosos en computadoras con Windows 7.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RIESGOS IDENTIFICADOS?

DESASTRES

PASO 1

En la hoja *"DES_MR"*, en la sección *"Identificación"*, registrar los riesgos identificados según la siguiente descripción:

	DATOS GENERALES			IDENTIFICACIÓN				
CODIGO DEL RIESGO	ORIGEN	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)	AMENAZA	VULNERABILIDAD	RIESGO	EFECTO	DESCRIPCIÓN DEL RIESGO
R 1 I_001	2	3	4	5	6	7	8	9

LEYENDA

1. Código generado automáticamente, tomando como referencia el código del proceso, el cual se selecciono en la cabecera del registro.

   RDE-PM01_001

   R: Riesgo, DE: Desastres — PM01: Código de proceso — Correlativo

2. Lista con opciones de origen (Contexto, Partes interesadas, provisión de productos y servicios y comunicación interna).
3. Producto (Nombre de producto de acuerdo a la definición de Gestión por Procesos, seleccionar el valor de la lista).
4. Producto (Nombre de productos priorizados informados a Contraloría, seleccionar el que corresponda de la lista.

LEYENDA

5. Describir brevemente la amenaza
6. Describir brevemente la vulnerabilidad.
7. Mencionar el riesgo.
8. Describir brevemente el efecto.
9. Describir el riesgo teniendo en cuenta los campos amenaza, vulnerabilidad, riesgo y efecto.

EJEMPLO

Debido a que se encuentra pendiente completar la implementación de medidas de prevención ante la ocurrencia de un sismo de gran magnitud o desastre en la ciudad de Lima, podría ocasionar muertes, así como, daños a la infraestructura, afectando la continuidad de las operaciones en la entidad.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RIESGOS IDENTIFICADOS?

INTEGRIDAD

PASO 1

En la hoja *"INT_MR"*, en la sección *"Identificación"*, registrar los riesgos identificados según la siguiente descripción:

	DATOS GENERALES		
CODIGO DEL RIESGO	ORIGEN	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)
R 1 I_001	2	3	4

IDENTIFICACIÓN						
ONTEXTO DEL RIESGO	POSIBLE COMPORTAMIENTO IRREGULAR	AGENTE	REDACCIÓN DEL RIESGO	TIPO DE RIESGO	CAUSA	EFECTO
CONTEXTO 1	POSIBLE COMPORTAMIENTO IRREGULAR 1	POTENCIAL AGENTE PRIMARIO				
1	2	3	4	5	6	7

LEYENDA

1. Código generado automáticamente, tomando como referencia el código del proceso, el cual se selecciono en la cabecera del registro.

   RIN-PM01_001

   R: Riesgo, IN: Integridad — PM01: Código de proceso — Correlativo

2. Lista con opciones de origen (Contexto, Partes interesadas, provisión de productos y servicios y comunicación interna).
3. Producto (Nombre de producto de acuerdo a la definición de Gestión por Procesos, seleccionar el valor de la lista).
4. Producto (Nombre de productos priorizados informados a Contraloría, seleccionar el que corresponda de la lista.

LEYENDA

1. Seleccionar el contexto
2. Seleccionar el posible comportamiento irregular
3. Definir el agente (persona o entidad que ocasiona el riesgo)
4. Describir el riesgo, considerando el agente y posible comportamiento irregular y el contexto.
5. Seleccionar el tipo de riesgo (corrupción o inconducta funcional).
6. Seleccionar la causa de la lista predefinida.
7. Describir el efecto.

EJEMPLO

El servidor civil de logística podría direccionar un proceso de compra de bienes o servicios a cambio de un soborno debido a falta o deterioro de carácter ético, ocasionando afectación en la reputación y credibilidad del proceso de contratación de proveedores en la entidad.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

HERRAMIENTAS PARA IDENTIFICACIÓN DE CAUSAS

Las herramientas de calidad, pueden ayudar a identificar la causa raíz de los riesgos:

- Ishikawa
- Lluvia de ideas
- Pareto
- 5 Porqués
- Diagrama de Flujo de Procesos
- Entre otros.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Análisis del Riesgo

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

ANÁLISIS DEL RIESGOS

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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RESULTADOS DEL ANÁLISIS?
OPERATIVO Y DESASTRES

PASO 2

En la hoja *"OPE_MR",* para riesgos Operativos y en hoja *"DES_MR"* para riesgos de Desastres en la sección *"Análisis",* registrar los resultados del análisis de los riesgos según la siguiente descripción:

ANÁLISIS									
ANÁLISIS DE PROBABILIDAD E IMPACTO			EVALUACIÓN DE CONTROL EXISTENTE						
PROBABILIDAD	IMPACTO	NIVEL DE EXPOSICIÓN DEL RIESGO INHERENTE	CONTROL EXISTENTE	1. Momento de su aplicación	2. Nivel de automatización	3. Periodicidad de aplicación	4. Responsabilidad	5. Documentación	6. Evidencia
1	2	3	4	5	6	7	8	9	10

LEYENDA

1. Seleccionar el nivel de probabilidad: Baja, Media, Alta y Muy Alta.
2. Seleccionar el nivel de impacto: Bajo, Medio, Alto y Muy Alto.
3. Visualizar el nivel de exposición del riesgo inherente, campo con fórmula.
4. Describir brevemente el control existente con mayor relevancia para mitigar el riesgo.
5. Criterio para evaluar el control "Momento de su aplicación", alternativas Preventiva y Correctiva.
6. Criterio para evaluar el control "Nivel de automatización", alternativas Automática y Manual.
7. Criterio para evaluar el control "Periodicidad de aplicación", alternativas Definida y No Definida.
8. Criterio para evaluar el control "Responsabilidad", alternativas Asignada y No asignada.
9. Criterio para evaluar el control "Documentación", alternativas Documentado y Sin documentar.
10. Criterio para evaluar el control "Evidencia", alternativas Con Registro y Sin registro.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RESULTADOS DEL ANÁLISIS?
SEGURIDAD DE LA INFORMACIÓN

PASO 2

En la hoja *"SIN_MR",* en la sección *"Análisis",* registrar los resultados del análisis de los riesgos según la siguiente descripción:

ANÁLISIS												
ANÁLISIS DE PROBABILIDAD E IMPACTO						EVALUACIÓN DEL CONTROL EXISTENTE						
PROBABILIDAD	CONFIABILIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	NIVEL DE EXPOSICIÓN DEL RIESGO INHERENTE	CONTROL EXISTENTE	1. Momento de su aplicación	2. Nivel de automatización	3. Periodicidad de aplicación	4. Responsabilidad	5. Documentación	6. Evidencia
1	2	3	4	5	6	7	8	9	10	11	12	13

LEYENDA

1. Seleccionar el nivel de probabilidad: Baja, Media, Alta y Muy Alta.
2. Seleccionar valor 1, 2 o 3 según corresponda, ver tablas de valoración del CID - confidencialidad, en hoja *"SIN_RE"*.
3. Seleccionar valor 1, 2 o 3 según corresponda, ver tablas de valoración del CID - integridad, en sección *"SIN_RE"*.
4. Seleccionar valor 1, 2 o 3 según corresponda, ver tablas de valoración del CID - disponibilidad, en sección *"SIN_RE"*.
5. Visualizar el valor CID, producto de la combinación de la valoración de los pilares (confidencialidad, integridad y disponibilidad), *campo contiene formula, no editar.*
6. Visualizar el nivel de exposición del riesgo inherente, campo con fórmula.
7. Describir brevemente el control existente con mayor relevancia para mitigar el riesgo.
8. Criterio para evaluar el control "Momento de su aplicación", alternativas Preventiva y Correctiva.
9. Criterio para evaluar el control "Nivel de automatización", alternativas Automática, Manual y N/A.
10. Criterio para evaluar el control "Periodicidad de aplicación", alternativas Definida y No Definida.
11. Criterio para evaluar el control "Responsabilidad", alternativas Asignada y No asignada.
12. Criterio para evaluar el control "Documentación", alternativas Documentado y Sin documentar.
13. Criterio para evaluar el control "Evidencia", alternativas Con Registro, Sin registro y N/A.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

TABLA DE VALORACIÓN CID

Tabla de Valoración de Confidencialidad

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

Tabla de Valoración de Integridad

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

Tabla de Valoración de Disponibilidad

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

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

CID

En la hoja *"SIN_RE"*, se puede visualizar las siguientes tablas con la explicación de los valores para probabilidad, impacto y nivel de riesgo.

Aspecto de Seguridad afectado por el riesgo			VALOR CID
Confidencialidad	Integridad	Disponibilidad	(IMPACTO)
1	1	1	Bajo
1	1	2	Bajo
1	1	3	Alto
1	2	1	Bajo
1	2	2	Medio
1	2	3	Alto
1	3	1	Alto
1	3	2	Alto
1	3	3	Muy Alto
2	1	1	Bajo
2	1	2	Medio
2	1	3	Alto
2	2	1	Medio
2	2	2	Medio
2	2	3	Alto
2	3	1	Alto
2	3	2	Alto
2	3	3	Muy Alto
3	1	1	Alto
3	1	2	Alto
3	1	3	Muy Alto
3	2	1	Alto
3	2	2	Alto
3	2	3	Muy Alto
3	3	1	Muy Alto
3	3	2	Muy Alto
3	3	3	Muy Alto

Resultado Fórmula	Nivel del Riesgo Inherente
Entre 80 al 100	MUY ALTO
Entre 48 al 64	ALTO
Entre 32 al 40	MEDIO
Entre 16 al 24	BAJO

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

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

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE SE REGISTRAN LOS RESULTADOS DEL ANÁLISIS?

INTEGRIDAD

PASO 2

En la hoja *"INT_MR",* en la sección *"Análisis",* registrar los resultados del análisis de los riesgos según la siguiente descripción:

ANÁLISIS									
ANÁLISIS DE PROBABILIDAD E IMPACTO			EVALUACIÓN DE CONTROL EXISTENTE						
PROBABILIDAD	IMPACTO	NIVEL DE EXPOSICIÓN DEL RIESGO INHERENTE	CONTROL EXISTENTE	1. Momento de su aplicación	2. Nivel de automatización	3. Periodicidad de aplicación	4. Responsabilidad	5. Documentación	6. Evidencia
1	2	3	4	5	6	7	8	9	10

LEYENDA

1. Seleccionar el nivel de probabilidad: Baja, Media, Alta y Muy Alta.
2. Seleccionar el nivel de impacto: Bajo, Medio, Alto y Muy Alto.
3. Visualizar el nivel de exposición del riesgo inherente, campo con fórmula.
4. Describir brevemente el control existente con mayor relevancia para mitigar el riesgo.
5. Criterio para evaluar el control "Momento de su aplicación", alternativas Preventiva y Correctiva.
6. Criterio para evaluar el control "Nivel de automatización", alternativas Automática, Manual y N/A.
7. Criterio para evaluar el control "Periodicidad de aplicación", alternativas Definida, No Definida y N/A.
8. Criterio para evaluar el control "Responsabilidad", alternativas Asignada y No asignada.
9. Criterio para evaluar el control "Documentación", alternativas Documentado y Sin documentar.
10. Criterio para evaluar el control "Evidencia", alternativas Con Registro y Sin registro.

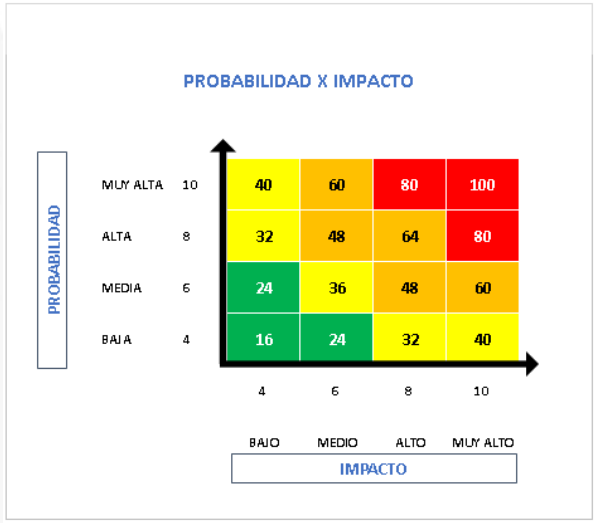
RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

COMBINA_NIVELEXPO

Nivel de Exposición	Valor de Exposición
Bajo	16
Bajo	24
Medio	32
Medio	36
Medio	40
Alto	48
Alto	60
Alto	64
Muy Alto	80
Muy Alto	100

Probabilidad	Valor Probabilidad	Impacto	Valor Impacto
Muy Alta	10	Muy Alto	10
Alta	8	Alto	8
Media	6	Medio	6
Baja	4	Bajo	4

Calificativo	Valor Controles	Probabilidad	Impacto
Excelente	12	Baja 1 nivel	Baja 1 nivel
Bueno	11	Baja 1 nivel	No Baja
Bueno	10	Baja 1 nivel	No Baja
Bueno	9	Baja 1 nivel	No Baja
Regular	8	No Baja	No Baja
Regular	7	No Baja	No Baja
Regular	6	No Baja	No Baja
Regular	5	No Baja	No Baja
Malo	4	No Baja	No Baja
Malo	3	No Baja	No Baja
Malo	2	No Baja	No Baja



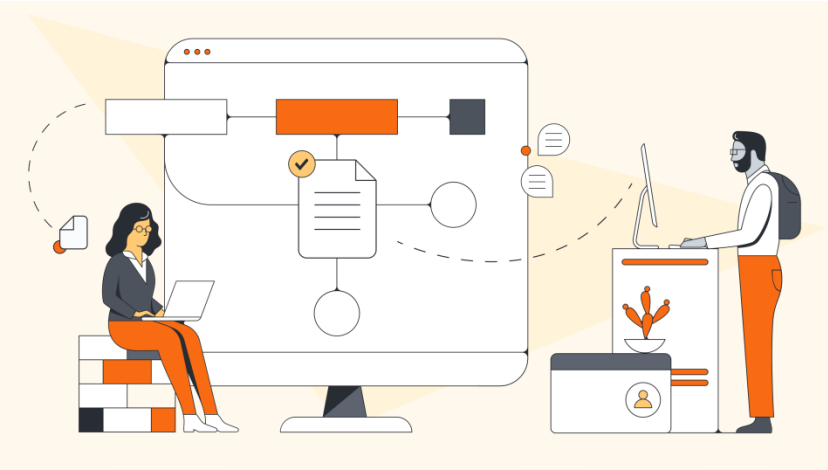
Probabilidad	Impacto	Valor Actual Nivel de Exposición	Nivel de Exposición	Calificativo Control Existente	Nueva Probabilidad	Nuevo Impacto	Nuevo Valor de Exposición	Nuevo Nivel de Exposición	Cambio
8	4	32	Medio	Excelente	6	4	24	Bajo	MEJORO
8	4	32	Medio	Bueno	6	4	24	Bajo	MEJORO
8	4	32	Medio	Regular	8	4	32	Medio	NO MEJORO
8	4	32	Medio	Malo	8	4	32	Medio	NO MEJORO
4	8	32	Medio	Excelente	4	6	24	Bajo	MEJORO
4	8	32	Medio	Bueno	4	8	32	Medio	NO MEJORO
4	8	32	Medio	Regular	4	8	32	Medio	NO MEJORO
4	8	32	Medio	Malo	4	8	32	Medio	NO MEJORO
6	6	36	Medio	Excelente	4	4	16	Bajo	MEJORO
6	6	36	Medio	Bueno	4	6	24	Bajo	MEJORO
6	6	36	Medio	Regular	6	6	36	Medio	NO MEJORO
6	6	36	Medio	Malo	6	6	36	Medio	NO MEJORO
10	4	40	Medio	Excelente	8	4	32	Medio	NO MEJORO
10	4	40	Medio	Bueno	8	4	32	Medio	NO MEJORO
10	4	40	Medio	Regular	10	4	40	Medio	NO MEJORO
10	4	40	Medio	Malo	10	4	40	Medio	NO MEJORO
6	8	48	Alto	Excelente	4	6	24	Bajo	MEJORO
6	8	48	Alto	Bueno	4	8	32	Medio	MEJORO
6	8	48	Alto	Regular	6	8	48	Alto	NO MEJORO
6	8	48	Alto	Malo	6	8	48	Alto	NO MEJORO
8	6	48	Alto	Excelente	6	4	24	Bajo	MEJORO
8	6	48	Alto	Bueno	6	6	36	Medio	MEJORO
8	6	48	Alto	Regular	8	6	48	Alto	NO MEJORO
8	6	48	Alto	Malo	8	6	48	Alto	NO MEJORO
6	10	60	Alto	Excelente	4	8	32	Medio	MEJORO
6	10	60	Alto	Bueno	4	10	40	Medio	MEJORO
6	10	60	Alto	Regular	6	10	60	Alto	NO MEJORO
6	10	60	Alto	Malo	6	10	60	Alto	NO MEJORO
10	6	60	Alto	Excelente	8	4	32	Medio	MEJORO
10	6	60	Alto	Bueno	8	6	48	Alto	NO MEJORO
10	6	60	Alto	Regular	10	6	60	Alto	NO MEJORO
10	6	60	Alto	Malo	10	6	60	Alto	NO MEJORO
8	8	64	Alto	Excelente	6	6	36	Medio	MEJORO
8	8	64	Alto	Bueno	6	8	48	Alto	NO MEJORO
8	8	64	Alto	Regular	8	8	64	Alto	NO MEJORO
8	8	64	Alto	Malo	8	8	64	Alto	NO MEJORO
8	10	80	Muy Alto	Excelente	6	8	48	Alto	MEJORO
8	10	80	Muy Alto	Bueno	6	10	60	Alto	MEJORO
8	10	80	Muy Alto	Regular	8	10	80	Muy Alto	NO MEJORO
8	10	80	Muy Alto	Malo	8	10	80	Muy Alto	NO MEJORO
10	8	80	Muy Alto	Excelente	8	6	48	Alto	MEJORO
10	8	80	Muy Alto	Bueno	8	8	64	Alto	MEJORO
10	8	80	Muy Alto	Regular	10	8	80	Muy Alto	NO MEJORO
10	8	80	Muy Alto	Malo	10	8	80	Muy Alto	NO MEJORO
10	10	100	Muy Alto	Excelente	8	8	64	Alto	MEJORO
10	10	100	Muy Alto	Bueno	8	10	80	Muy Alto	NO MEJORO
10	10	100	Muy Alto	Regular	10	10	100	Muy Alto	NO MEJORO
10	10	100	Muy Alto	Malo	10	10	100	Muy Alto	NO MEJORO

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Valoración del Riesgo

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿CÓMO DETERMINO LA EFECTIVIDAD DEL CONTROL EXISTENTE?

PASO 3

En las hojas: *"OPE_MR", "SIN_MR", "DES_MR" y "INT_MR"*, visualizar el resultado de la valoración del control de acuerdo al análisis realizado.

VALORACIÓN				
NIVEL DE LA EFECTIVIDAD DEL CONTROL EXISTENTE	PROBABILIDAD ESPERADA	IMPACTO ESPERADO	NIVEL DE EXPOSICIÓN DEL RIESGO RESIDUAL (ANTES DEL TRATAMIENTO)	OPCIONES DE TRATAMIENTO AL RIESGO
1	2	3	4	5

LEYENDA

Todos los campos con fórmula, no editar.

Visualizar el resultado de los siguientes campos:

1. Nivel de la efectividad del control existente: Es la calificación de la evaluación del control existente, de acuerdo a los resultados de los criterios evaluados en la sección análisis. puede ser: Excelente, Bueno, Regular y Malo, este campo no se edita porque está con formula.
2. Probabilidad esperada: Si el control es "Bueno" o "Excelente", y la probabilidad es diferente de Baja, disminuye un nivel.
3. Impacto esperado: Se mantiene el mismo impacto de la sección análisis.
4. Nivel de exposición del riesgo residual (antes del tratamiento): Es el resultado de la multiplicación de los valores de la probabilidad esperada e impacto esperado.

5. Seleccionar la opción de tratamiento: Aceptar, Reducir, Evitar, Compartir.

OPCIÓN DE TRATAMIENTO RIESGO	
ACEPTAR	No se realiza ninguna acción adicional.
REDUCIR	Se debe implementar controles adicionales o mejorar los existentes a fin de reducir el nivel de riesgo.
EVITAR	Se dispone que no se inicie o continúe con la actividad que genera el riesgo.
COMPARTIR	Se dispone que control adicional sea realizado por un externo, bajo la supervisión del RENIEC. Ejemplo: Compañía de Seguros, proveedor especializado, etc.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

EVALUACIÓN DE LA EFECTIVIDAD DEL CONTROL (MEDIDAS DE CONTROL)

CRITERIO	CARACTERÍSTICA	DESCRIPCIÓN	PUNTAJE
1. Momento de su aplicación	Preventiva	Antes de que se materialice el hecho y afecta el proceso, actividad o activo.	2
	Correctiva	Después de que se materialice el hecho y afecta el proceso, actividad o activo.	1
2. Nivel de automatización	Automática	La medida se aplica usando la infraestructura tecnológica o los sistemas informáticos. También se considera actividades semiautomáticas.	2
	Manual	La medida no usa sistemas informáticos y se usan listas de cotejo, informes de verificación, herramientas en MS Excel, etc.	1
	N/A	No aplica criterio. (**)	2
3. Periodicidad de aplicación	Definido	Se ha establecido frecuencia de aplicación del control.	2
	No definido	No se ha establecido frecuencia de aplicación del control.	0
	N/A	No aplica criterio. (**)	2
4. Responsabilidad	Asignada	Existen responsables y funciones definidas.	2
	No asignada	No se ha determinado funciones ni se ha definido responsable.	0
5. Documentación	Documentado	Existe información documentada que acredita la definición del control.	2
	Sin Documentar	No existe información documentada que demuestre la definición del control.	0
6. Evidencia	Con Registro	Existe un registro que permite evidenciar la aplicación del control.	2
	Sin Registro	No existe registro de la aplicación del control.	0
	N/A	No aplica criterio. (*)	2
		PUNTAJE TOTAL	**12**

(*) Solo aplica para riesgos de Seguridad de la Información
(**) Aplica para riesgos de Seguridad de la Información y Riesgos que afecta a la Integridad Pública

NIVEL DE EFECTIVIDAD		
EXCELENTE	12	Medida de Control, si mitigará significativamente los riesgos. El valor de probabilidad e impacto, se reduce en un nivel.
BUENO	[9 - 11]	Medida de Control, si mitigará los riesgos. El valor de probabilidad, se reduce en un nivel.
REGULAR	[5 - 8]	Medida de Control, si mitigará en parte los riesgos identificados. Se recomienda revisar la medida de control e implementar mejoras al mismo.
MALO	[2 - 4]	Medida de control, no mitigará significativamente los riesgos. Se recomienda cambiar de medida de control.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Tratamiento del Riesgo

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

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.

SEGURIDAD DE LA INFORMACIÓN

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

ANTICORRUPCIÓN

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.

TRATAMIENTO – MEDIDAS DE CONTROL

PASO 4

En las hojas *"OPE_MC", "SIN_MC", "DES_MC" y "INT_MC",* se registra las medidas de control para riesgos que requieren tratamiento. Se puede registrar como máximo 3 medidas de control.
Según metodología, los riesgos con nivel de exposición ***MEDIO***, ***ALTO*** y ***MUY ALTO*** deben ser tratados.

	MEDIDA DE CONTROL 1						EVALUACIÓN							
CODIGO DEL RIESGO	MEDIDA DE CONTROL	ORGANO RESPONSABLE	FECHA DE INICIO DE IMPLEMENTACIÓN	FECHA FIN DE IMPLEMENTACIÓN	MEDIOS DE VERIFICACIÓN	ESTADO	1. Momento de su aplicación	2. Nivel de automatización	3. Periodicidad de aplicación	4. Responsabilidad	5. Documentación	6. Evidencia	VALOR DE LA EFECTIVIDAD	NIVEL DE LA EFECTIVIDAD DEL CONTROL IMPLEMENTADO
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

LEYENDA

1. Colocar el código del riesgo del que se va a realizar tratamiento y los siguientes campos de las secciones de datos generales, identificación y valoración se visualizará la información registrada en la hoja OPE_MR, SIN_MR, DES_MR e INT_MR.
2. Describir brevemente la medida de control a implementar con mayor relevancia para mitigar el riesgo. En el caso el riesgo es de seguridad de la información, seleccionar los campos de controles de la ISO 27001.
3. Registrar el órgano responsable de implementar la medida de control.
4. Registrar la fecha planificada de inicio de implementación de la medida de control.
5. Registrar la fecha planificada de término de implementación de la medida de control.
6. Registrar los medios de verificación con los cuales se comprobará la implementación de la medida de control.
7. Seleccionar el estado de la medida de control: Pendiente, En Proceso e Implementada.
8. Criterio para evaluar el control "Momento de su aplicación", alternativas Preventiva y Correctiva.
9. Criterio para evaluar el control "Nivel de automatización", alternativas Automática, Manual. (N/A para riesgos de Seguridad de la Información y riesgos que afecta a la Integridad Pública).
10. Criterio para evaluar el control "Periodicidad de aplicación", alternativas Definida, No Definida. (N/A para riesgos de Seguridad de la Información y riesgos que afecta a la Integridad Pública).
11. Criterio para evaluar el control "Responsabilidad", alternativas Asignada y No asignada.
12. Criterio para evaluar el control "Documentación", alternativas Documentado y Sin documentar.
13. Criterio para evaluar el control "Evidencia", alternativas Con Registro y Sin registro. . (N/A para riesgos de Seguridad de la Información).
14. Valor de la efectividad: Es el puntaje obtenido por la evaluación del control implementado.
15. Nivel de la efectividad del control existente: Es la calificación de la evaluación del control implementado, puede ser: Excelente, Bueno, Regular y Malo, este campo no se edita porque está con formula.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

TRATAMIENTO – ACCIONES

PASO 4

En las hojas *"OPE_AC", "SIN_AC", "DES_AC" y "INT_AC",* se registra las acciones por cada medida de control definida. Se puede registrar como máximo 3 medidas de control.
Según metodología, los riesgos con nivel de exposición ***MEDIO***, ***ALTO*** y ***MUY ALTO*** deben ser tratados.

DATOS GENERALES						IDENTIFICACIÓN	VALORACIÓN	TRATAMIENTO					
								MEDIDA DE CONTROL	ACCIONES				
CODIGO DEL RIESGO	ORIGEN	CATEGORÍA DE RIESGO	TIPO DE RIESGO	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)	DESCRIPCIÓN DEL RIESGO	NIVEL DE EXPOSICIÓN DEL RIESGO RESIDUAL (ANTES DEL TRATAMIENTO)	CONTROL PROPUESTO	ACCIONES	ORGANO RESPONSABLE	FECHA DE INICIO DE IMPLEMENTACIÓN	FECHA FIN DE IMPLEMENTACIÓN	MEDIOS DE VERIFICACIÓN
1	-	-	-	-	-	-	-	2	3	4	5	6	7

LEYENDA

1. Colocar el código del riesgo del que se va a realizar tratamiento y los siguientes campos de las secciones de datos generales, identificación y valoración se visualizará la información registrada en las hojas OPE_MR, SIN_MR, DES_MR e INT_MR. Se copiará el código de riesgo según el número de acciones que se registre por cada medida de control.
2. Copiar la medida de control registrada en las hojas: OPE_MC, SIN_MC, DES_MC e INT_MC.
3. Registrar la acción a implementar por la medida de control registrada.
4. Registrar el órgano responsable de implementar la acción.
5. Registrar la fecha planificada de inicio de implementación de la acción.
6. Registrar la fecha planificada de término de implementación de la acción.
7. Registrar los medios de verificación con los cuales se comprobará la implementación de la acción.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

EVALUACIÓN DE LA EFECTIVIDAD DEL CONTROL (MEDIDAS DE CONTROL)

CRITERIO	CARACTERÍSTICA	DESCRIPCIÓN	PUNTAJE
1. Momento de su aplicación	Preventiva	Antes de que se materialice el hecho y afecta el proceso, actividad o activo.	2
	Correctiva	Después de que se materialice el hecho y afecta el proceso, actividad o activo.	1
2. Nivel de automatización	Automática	La medida se aplica usando la infraestructura tecnológica o los sistemas informáticos. También se considera actividades semiautomáticas.	2
	Manual	La medida no usa sistemas informáticos y se usan listas de cotejo, informes de verificación, herramientas en MS Excel, etc.	1
	N/A	No aplica criterio. (**)	2
3. Periodicidad de aplicación	Definido	Se ha establecido frecuencia de aplicación del control.	2
	No definido	No se ha establecido frecuencia de aplicación del control.	0
	N/A	No aplica criterio. (**)	2
4. Responsabilidad	Asignada	Existen responsables y funciones definidas.	2
	No asignada	No se ha determinado funciones ni se ha definido responsable.	0
5. Documentación	Documentado	Existe información documentada que acredita la definición del control.	2
	Sin Documentar	No existe información documentada que demuestre la definición del control.	0
6. Evidencia	Con Registro	Existe un registro que permite evidenciar la aplicación del control.	2
	Sin Registro	No existe registro de la aplicación del control.	0
	N/A	No aplica criterio. (*)	2
		PUNTAJE TOTAL	**12**

(*) Solo aplica para riesgos de Seguridad de la Información
(**) Aplica para riesgos de Seguridad de la Información y Riesgos que afecta a la Integridad Pública

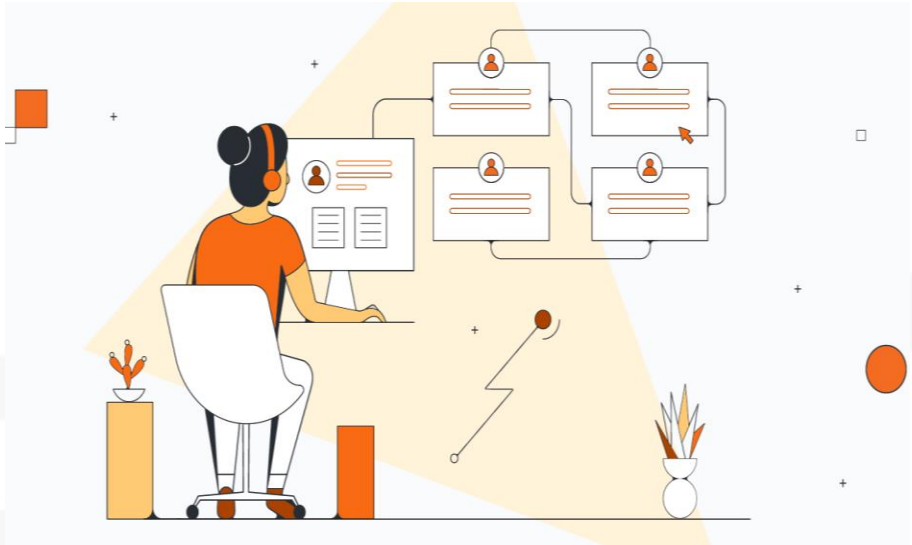
NIVEL DE EFECTIVIDAD		
EXCELENTE	12	Medida de Control, si mitigará significativamente los riesgos. El valor de probabilidad e impacto, se reduce en un nivel.
BUENO	[9 - 11]	Medida de Control, si mitigará los riesgos. El valor de probabilidad, se reduce en un nivel.
REGULAR	[5 - 8]	Medida de Control, si mitigará en parte los riesgos identificados. Se recomienda revisar la medida de control e implementar mejoras al mismo.
MALO	[2 - 4]	Medida de control, no mitigará significativamente los riesgos. Se recomienda cambiar de medida de control.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Seguimiento y Revisión

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

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 la ***PLAN DE GESTIÓN INTEGRAL DEL RIESGO 2023*** 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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO EL RESULTADO DEL SEGUIMIENTO MENSUAL?

PASO 5

En las hojas *"OPE_AC", "SIN_AC", "DES_AC" y "INT_AC",* revisar las acciones definidas por cada control propuesto y registrar comentarios del seguimiento realizado en el mes.

SEGUIMIENTO DEL PROCESO											
ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE VISUALIZARÉ EL RESULTADO DEL SEGUIMIENTO MENSUAL?

PASO 6

En las hojas *"OPE_AC", "SIN_AC", "DES_AC" y "INT_AC",* revisar las acciones definidas por cada control propuesto y los comentarios del responsable de supervisión.

Esta sección será completada por el responsable de supervisión:

SEGUIMIENTO DEL RESPONSABLE DE SUPERVISIÓN													
ESTADO	% AVANCE	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
1	2	3											

1. Seleccionar el estado de la acción, cada vez que se realice seguimiento, los estados pueden ser Pendiente, En Proceso e Implementada.
2. Registrar el porcentaje de avance, de acuerdo a las evidencias presentadas.
3. Registrar comentarios de la revisión (resumen) en el mes que corresponda.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

REGISTRO E INFORME

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS ACCIONES POR CONTROL PROPUESTO?

PASO 7

Ir a la hoja *"MEJ"*, mensualmente reportar la problemática y recomendaciones de mejora identificadas por cada producto. A continuación, las 2 secciones:

RECOMENDACIONES DE MEJORA

A

AÑO	2023	FECHA DE APROBACIÓN	15/06/2023
NOMBRE DEL PROCESO	PM01_PROCESO DE LA IDENTIFICACION		

B

PROBLEMÁTICA Y RECOMENDACIONES								
CÓDIGO	MES	PRODUCTO (GESTIÓN POR PROCESOS)	PRODUCTO (PROGRAMA PRESUPUESTAL)	PROBLEMÁTICA	RECOMENDACIONES DE MEJORA	FECHA PROPUESTA DE IMPLEMENTACIÓN DE LA MEJORA	MEDIO DE VERIFICACIÓN	SEGUIMIENTO
PM01_RM01	Mayo							

- Los campos año y nombre del proceso se visualizan de los datos registrados en las hojas anteriores.
- Se registra la fecha de aprobación.

- Seleccionar el mes, producto y registrar problemáticas y recomendaciones de mejora por mes y por producto.
- Registrar fecha propuesta de implementación y medio de verificación.
- La información de seguimiento lo registrará el responsable de supervisión.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PASO 8

Ir a la hoja ***"REP"***, visualizar las cantidades por cada tipo de riesgo, nivel de riesgo inherente, nivel de riesgo residual, implementación de controles y su efectividad en el tratamiento.

Asimismo, visualizar la gráficas, y completar un comentario en el campo A y B.

Todos los campos se encuentran con fórmula, NO editar.

REPORTE DE ESTADO DE GESTIÓN INTEGRAL DE RIESGOS

AÑO	2023	MES	6

PROCESO	PM01_PROCESO DE LA IDENTIFICACION

CANTIDAD RIESGOS POR SU CLASIFICACIÓN	DESEMPEÑO			INTEGRIDAD	
	Desastres	Operativo	Seguridad de la Información	Corrupción	Inconducta Funcional
Cantidad de Riesgos	0	0	0	0	0
TOTAL	0				

NIVEL DE RIESGO INHERENTE	DESEMPEÑO			INTEGRIDAD	
	Desastres	Operativo	Seguridad de la Información	Corrupción	Inconducta Funcional
Muy Alto	0	0	0	0	0
Alto	0	0	0	0	0
Medio	0	0	0	0	0
BAJO	0	0	0	0	0
TOTAL	0	0	0	0	0

NIVEL DE RIESGO RESIDUAL ANTES DEL TRATAMIENTO	DESEMPEÑO			INTEGRIDAD	
	Desastres	Operativo	Seguridad de la Información	Corrupción	Inconducta Funcional
Muy Alto	0	0	0	0	0
Alto	0	0	0	0	0
Medio	0	0	0	0	0
Bajo	0	0	0	0	0
TOTAL	0	0	0	0	0

NIVEL DE RIESGO RESIDUAL DESPUES DEL TRATAMIENTO	DESEMPEÑO			INTEGRIDAD	
	Desastres	Operativo	Seguridad de la Información	Corrupción	Inconducta Funcional
Muy Alto	0	0	0	0	0
Alto	0	0	0	0	0
Medio	0	0	0	0	0
Bajo	0	0	0	0	0
TOTAL	0	0	0	0	0

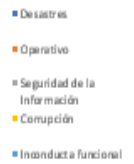
A

REPORTE DE ESTADO DE GESTIÓN INTEGRAL DE RIESGOS

AÑO	2023	MES	6	PROCESO	PM01_PROCESO DE LA IDENTIFICACION

RESUMEN DE RIESGOS

TIPO DE RIESGOS



B

RIESGOS DE DESEMPEÑO

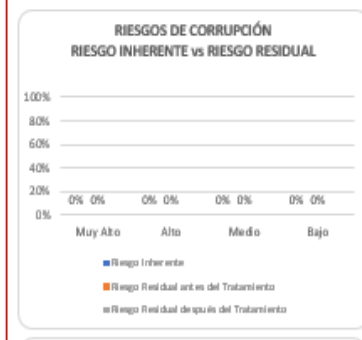
RIESGOS OPERATIVOS
RIESGO INHERENTE vs RIESGO RESIDUAL

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN RIESGO INHERENTE vs RIESGO RESIDUAL

RIESGOS DE DESASTRES
RIESGO INHERENTE vs RIESGO RESIDUAL

RIESGOS DE INTEGRIDAD

RIESGOS DE CORRUPCIÓN
RIESGO INHERENTE vs RIESGO RESIDUAL



RIESGOS DE INCONDUCTA FUNCIONAL
RIESGO INHERENTE vs RIESGO RESIDUAL

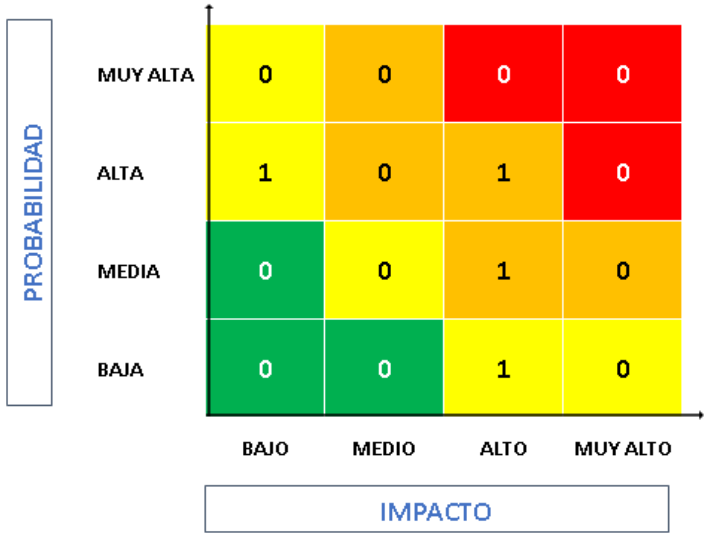
RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE VISUALIZO LOS RIESGOS?

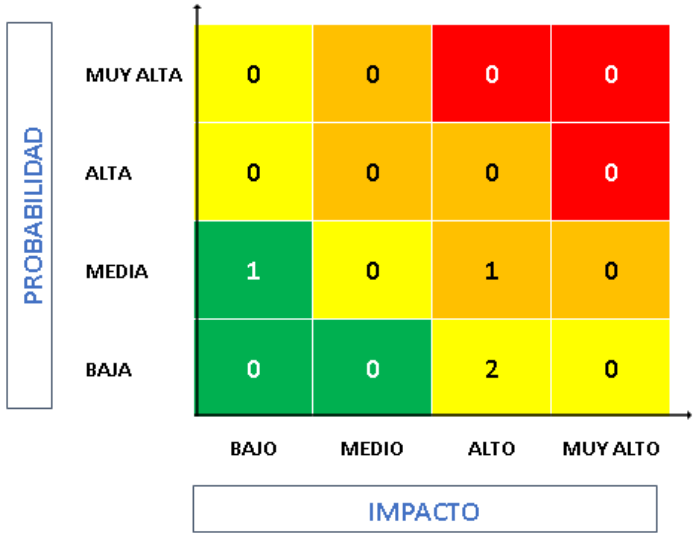
PASO 9

Ir a la hoja *"MRI"*, y visualizar la cantidad de riesgos por cuadrante, según su nivel de exposición, *campo contiene fórmulas, NO modificar*. Asimismo, se tiene mapa de riesgos a nivel general y para los riesgos operativos, seguridad de la información, desastres y riesgos que afectan la integridad pública.

MAPA DE RIESGOS
(Antes del Tratamiento)



MAPA DE RIESGOS
(Después del Tratamiento)



RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

GESTIÓN DE OPORTUNIDADES

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DE QUÉ PROCESO ESTOY GESTIONANDO LA OPORTUNIDAD?

PASO 0

En todas las hojas de registro de la herramienta se cuenta con la siguiente cabecera.

VERSIÓN	1	2.0	FECHA DE APROBACIÓN	2	15/06/2023
PROCESO	3	PM01_PROCESO DE LA IDENTIFICACION	TIPO DE PROCESO	4	MISIONAL
ÓRGANO DUEÑO DEL PROCESO	5	Dirección de Registro de Identificación	ÓRGANOS QUE PARTICIPAN EN EL PROCESO	6	DRI, DRIAS, DSR

LEYENDA

1. Versión: Colocar el número de versión.
2. Fecha de aprobación: Registrar la fecha de aprobación por el Dueño de Proceso en formato dd/mm/aaaa.
3. Proceso: Seleccionar el proceso del cual se va a gestionar riesgos.
4. Tipo de Proceso: Campo con fórmula, No editar, al seleccionar el proceso, se visualizará si es misional, soporte o estratégico.
5. Órgano Dueño del Proceso: Seleccionar el órgano que dirige el dueño del proceso.
6. Órganos que participan en el proceso: Registrar los órganos que participan en el proceso, incluyendo al órgano del dueño de proceso, en siglas.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS OPORTUNIDADES?

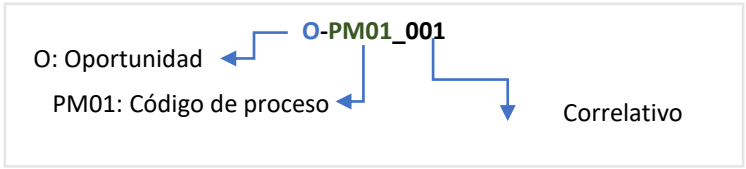
PASO 1

Ir al archivo *PGO*, ver hoja *"MO"*, registrar la información en los campos en blanco.

	DATOS GENERALES			IDENTIFICACIÓN	
CODIGO DE LA OPORTUNIDAD	ORIGEN	TIPO DE OPORTUNIDAD	PRODUCTO (GESTIÓN POR PROCESOS)	DESCRIPCIÓN DE LA OPORTUNIDAD	BENEFICIOS
1	2	3	4	5	6
O-PM02-001	Provisión de productos o servicio	Servicio	Acta registral procesada	Descripción de oportunidad 1	

LEYENDA

1. Código generado automáticamente, tomando como referencia el código del proceso, el cual se selecciono en la cabecera del registro.



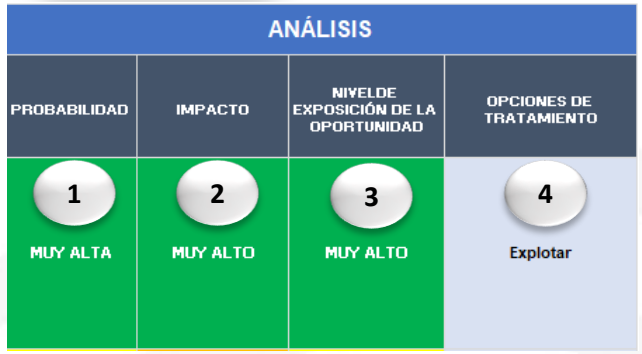
2. Lista con opciones de origen (contexto, partes interesadas, ejecución del servicio y comunicación interna).
3. Seleccionar el tipo oportunidad: servicio, legal, tecnológico y gestión.
4. Seleccionar el tipo de producto (Nombre de producto de acuerdo a Gestión por Procesos).
5. Describir brevemente la oportunidad.
6. Listar los beneficios (efecto), que se obtiene al implementar la oportunidad.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS OPORTUNIDADES?

PASO 2

Ir al archivo *PGO*, ver hoja *"MO"*, registrar la información en los campos en blanco.



LEYENDA

10. Seleccionar la probabilidad de ocurrencia de la oportunidad (baja, media, alta y muy alta).
11. Visualizar el valor de probabilidad: (baja:4, media:6, alta:8 y muy alta:10).
12. Seleccionar el nivel de impacto, (bajo, medio, alto y muy alto).
13. Se visualiza el valor del impacto (bajo:4, medio:6, alto:8 y muy alto:10).
14. Se visualiza el valor de la oportunidad.
15. Se visualiza el nivel de exposición de la oportunidad.
16. Seleccionar respuesta de tratamiento (aceptar, reducir, evitar o compartir).

Clasificación	Nivel	Descripción
MUY ALTA	10	Es inminente que la oportunidad se concrete.
ALTA	8	La oportunidad podría realizarse, existen condiciones que hacen posible la realización en un corto plazo.
MEDIA	6	La oportunidad podría realizarse, existen condiciones que hacen posible la realización en un mediano plazo.
BAJA	4	La oportunidad podría realizarse, existen condiciones que hacen posible la realización en un largo plazo.

Clasificación	Nivel	Descripción
MUY ALTA	10	Su implementación tendría un efecto duradero que beneficiaría al proceso, generando resultados muy superiores a los esperados en el logro de sus objetivos.
ALTA	8	Su implementación tendría un efecto prolongado que beneficiaría al proceso, generando resultados esperados en el logro de sus objetivos.
MEDIA	6	Su implementación tendría un impacto directo en el proceso y el efecto es temporal, podría generar los resultados esperados en el logro de sus objetivos.
BAJA	4	La oportunidad tiene impacto indirecto en el proceso.

RESPUESTA	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.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

TRATAMIENTO – ACCIONES

PASO 3

En las hoja *"AS"*, se registra las acciones por cada oportunidad.
Según metodología, los riesgos con nivel de exposición ***MEDIO***, ***ALTO*** y ***MUY ALTO*** deben ser tratados.

IDENTIFICACIÓN				ACCIONES				
CODIGO DEL RIESGO	TIPO DE OPORTUNIDAD	PRODUCTO (GESTIÓN POR PROCESOS)	DESCRIPCIÓN DE LA OPORTUNIDAD	ACCIONES	ORGANO RESPONSABLE	FECHA DE INICIO DE IMPLEMENTACIÓN	FECHA FIN DE IMPLEMENTACIÓN	MEDIOS DE VERIFICACIÓN
1	Servicio	Acta registral procesada	Descripción de oportunidad 1	2	3	4	5	6

LEYENDA

1. Colocar el código de la oportunidad del que se va a realizar tratamiento y en los siguientes campos de las sección identificación se visualizará la información registrada en la hoja MO.
2. Registrar la acción a implementar por cada oportunidad registrada.
3. Registrar el órgano responsable de implementar la acción.
4. Registrar la fecha planificada de inicio de implementación de la acción.
5. Registrar la fecha planificada de término de implementación de la acción.
6. Registrar los medios de verificación con los cuales se comprobará la implementación de la acción.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS OPORTUNIDADES?

PASO 4

Ir al archivo *PGO*, ver hoja *"AS"*, revisar las acciones definidas por cada oportunidad y registrar comentarios del seguimiento realizado en el mes y seleccionar estado de acción.

SEGUIMIENTO DEL PROCESO												
ESTADO	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE

- Seleccionar el estado de la acción, cada vez que se realice seguimiento, los estados pueden ser Pendiente, En Proceso e Implementada, campo 48.
- Registrar actividades ejecutadas (resumen) en el mes que corresponda.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS OPORTUNIDADES?

PASO 5

Ir al archivo ***PGO***, ver hoja ***"AS"***, revisar las acciones definidas por cada control propuesto y los comentarios de OIR.

Esta sección será completada por el responsable de supervisión:

SEGUIMIENTO DEL RESPONSABLE DE SUPERVISIÓN													
ESTADO	% AVANCE	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
1	2	3											

1. Seleccionar el estado de la acción, cada vez que se realice seguimiento, los estados pueden ser Pendiente, En Proceso e Implementada.
2. Registrar el porcentaje de avance, de acuerdo a las evidencias presentadas.
3. Registrar comentarios de la revisión (resumen) en el mes que corresponda.

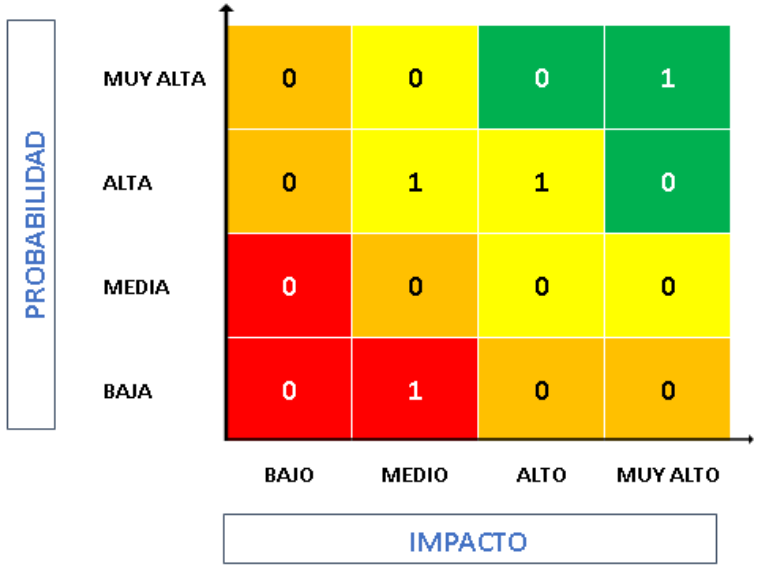
RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿DÓNDE REGISTRO LAS OPORTUNIDADES?

PASO 6

Ir a la hoja *"PGO"*, y visualizar la cantidad de oportunidades por cuadrante, según su nivel de exposición, *campo contiene fórmulas, NO modificar*.

MAPA DE OPORTUNIDADES



RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

ANEXO: MEDIDAS DE CONTROL

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

¿Qué son las medidas de control y cómo las definimos?

"De acuerdo con la Directiva de la CGR las medidas de control pueden ser definidas como las políticas, procedimientos, técnicas y otros mecanismos que permitan reducir los riesgos. Por cada riesgo que debe recibir tratamiento (según la evaluación de riesgos), se definen las medidas de control, que son la forma en que las entidades hacen frente a sus posibles riesgos."

Fuente: Guía de Gestión de Riesgos de Contraloría

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Figura 5.2. Respuestas a riesgos según tipo de causa

Causas internas	• Medida de control orientada a las causas del riesgo • Medida de control orientada a mejorar la capacidad de respuesta de la entidad
Causas externas que competen a la entidad	• Medida de control orientada a las causas del riesgo • Medida de control orientada a mejorar la capacidad de respuesta de la entidad • Supervisar a un tercero, si se ha compartido el riesgo
Causas externas fuera del control de la entidad	• Monitorear la situación • Informar a la instancia superior y/o rector competente • Medida de control orientada a mejorar la capacidad de respuesta de la entidad

Recuerda

Por cada causa identificada, la entidad puede definir una o más medidas de control.

Recuerda

Si bien las causas del riesgo no se ingresan en el aplicativo informático del SCI, es importante que la entidad las registre en documentos internos, como sustento de las razones por las cuales se estableció una medida de control determinada.

Ello es necesario, además, debido a la alta rotación de personal.

Fuente: Guía de Gestión de Riesgos de Contraloría

Cuadro 5.2. Ejemplos de medidas de control según su orientación

Para evitar las causas	Para mejorar la capacidad de respuesta de la entidad
▪ **Supervisar** el desarrollo de planes de mantenimiento preventivo	▪ **Supervisar** el desarrollo de planes de mantenimiento correctivo
▪ **Inspeccionar** o realizar visitas de inspección programadas	▪ **Inspeccionar** o realizar visitas de inspección no programadas (inopinadas)
▪ **Aplicar** listas de chequeo (o chequear)	▪ **Contrastar** información para identificar diferencias (conciliar)
▪ **Aplicar** doble verificación o aprobación (control dual)	▪ **Retroalimentar** a través de comités o reuniones periódicas
▪ **Verificar** la ejecución de programas de capacitación	▪ **Evaluar** el desempeño de los/as servidores/as capacitados/as
▪ **Activar alertas** de sistemas de información	▪ **Verificar** que se cuente con respaldos de información (*backups*)
▪ **Efectuar seguimiento** a cronogramas o planes de trabajo ▪ **Efectuar seguimiento** o aplicar protocolos o guías	▪ **Ejecutar** planes de contingencia o protocolos de emergencia
▪ **Separar** funciones para cada puesto (segregación) en el proceso de contratación de bienes y servicios	▪ **Realizar** autoevaluaciones

Fuente: Guía de Gestión de Riesgos de Contraloría

Ejemplo 1: Definición de medidas de control - Red de salud

En este ejemplo, se identificaron dos causas. Con respecto a la primera, vemos que la medida de control se ha redactado incluyendo en cursiva el texto que se refiere a su objetivo. La red de salud busca asegurar la actualización permanente del registro porque se analizó que una causa del riesgo era que este se encontraba desactualizado, lo cual dificultaba conocer el número de atenciones CRED realizadas de acuerdo con la edad del niño o de la niña.

Riesgo: CRED podría brindarse sin cumplir el número de atenciones definido, de acuerdo con la edad del niño o de la niña.

Tipo de causa	Causa 1	Actor de la causa
Interna	Información desactualizada en el sistema informático correspondiente	Establecimiento de salud

Medida de control

Verificar el registro oportuno de las atenciones del CRED en el sistema informático correspondiente, *a fin de asegurar su actualización permanente* (*).

Nota (*): Se ha escrito con cursiva la finalidad de la medida de control para vincularla con la causa.

Para el mismo riesgo, se identificó como causa externa "padrón nominal de niños y niñas menores de tres años con información desactualizada". Estrictamente, la red de salud no puede evitar la causa. Sin embargo, como los establecimientos de salud participan en el proceso de validación y actualización de la información con otros actores, se plantea que la red de salud verifique la entrega oportuna de información a las municipalidades, por parte de los establecimientos de salud a su cargo.

Tipo de causa	Causa 2	Actor de la causa
Externa	Padrón nominal de niños y niñas menores de tres años con información desactualizada	Establecimiento de salud y municipalidad

Medida de control

Verificar la entrega oportuna de información de niños y niñas nuevos a las municipalidades para su registro en el padrón nominal y su homologación respectiva, *a fin de asegurar la actualización permanente del padrón* (*).

Nota (*): Se ha escrito con cursiva la finalidad de la medida de control para vincularla con la causa.

Fuente: Guía de Gestión de Riesgos de Contraloría

PP1

Riesgo: Debido a deficiencias en la estrategia de entrega de DNI a la población podría ocurrir que los ciudadanos no se presenten en la fecha y hora programada para la campaña de documentación itinerante ocasionando la afectación al ciudadano al no recibir su DNI.

Tipo de causa	causa	Actor de la causa
Interna	Deficiencias en la entrega de DNI en campañas itinerantes.	Encargado de coordinar entrega de DNI

Medida de control

Verificar que las actividades programadas con otras áreas o entidades, se realicen según lo planificado.

Medida de control

Efectuar seguimiento a la entrega de DNI en campañas itinerantes.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PP2

Riesgo: El responsable de almacén podría realizar un retiro no autorizado de suministros en beneficio propio, afectando la disponibilidad de recursos en la entidad.

Tipo de causa	causa	Actor de la causa
Interna	Falta o deterioro del carácter ético	Responsable de almacén

Medida de control

Implementar mecanismo de recordatorios sobre valores y conductas deseables al personal de almacén.

Medida de control

Verificar inventario de suministros con el registro de ingresos y salidas (Kardex) corresponda con lo solicitado por usuarios.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PP3

Riesgo: Debido a la falta de un proveedor alterno del servicios de internet, puede ocurrir la perdida de conectividad a internet, lo que ocasionaría que los servicios de certificación digital que brinda RENIEC se vean interrumpidos.

Tipo de causa	causa	Actor de la causa
Interna	Falta de proveedor alterno del servicio de internet	Personal encargado contratar proveedor

Medida de control

Verificar que el protocolo de cambio al proveedor alterno se ejecute como contingencia.

Medida de control

Supervisar el desarrollo de planes de mantenimiento preventivo.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL


RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL