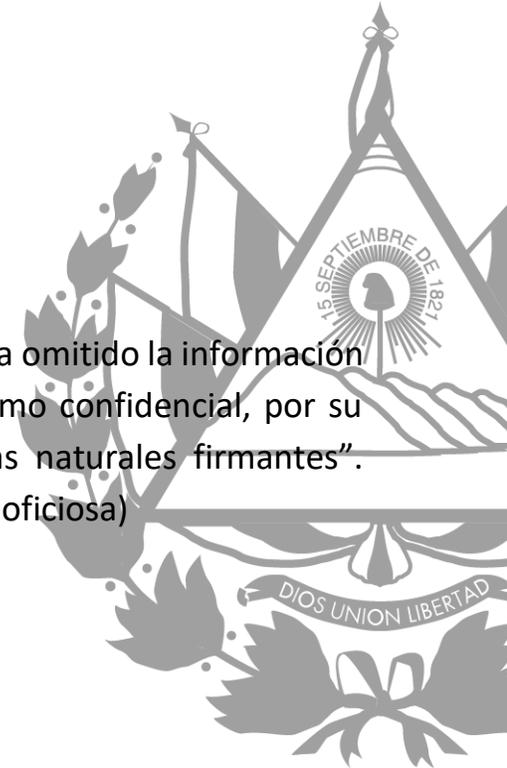




VERSIÓN PÚBLICA

“Este documento es versión pública, por lo que, únicamente se ha omitido la información que la Ley de Acceso a la Información Pública (LAIP) define como confidencial, por su carácter privado tales como datos personales de las personas naturales firmantes”.
(Artículo 24 y 30 de la LAIP para la publicación de la información oficiosa)



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 1 de 25	

MANUAL DE GESTIÓN DE RIESGOS INSTITUCIONAL

			
Sello	Sello	Sello	Acuerdo: 27.15 Acta: 47 Extraordinaria 28/11/2024
Técnico de Gestión de la Calidad Institucional	Director de Planificación	Gerente General	JUNTA DIRECTIVA
Elaboró	Revisó	Visto Bueno	Aprobó

	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
Manual de Gestión de Riesgos Institucional		Fecha de emisión:	27/11/2024
		Página 2 de 25	

INDICE

SIGLAS Y ABREVIATURAS	3
INTRODUCCIÓN.....	3
OBJETIVOS	3
OBJETIVO GENERAL.....	3
OBJETIVOS ESPECIFICOS	3
TERMINOLOGÍA.....	4
ALCANCE	5
CAMPO DE APLICACIÓN.....	5
NORMATIVA INTERNA.....	5
GESTIÓN DE RIESGOS	6
FUNCIONES Y RESPONSABILIDADES PARA LA GESTIÓN DE RIESGOS	6
CONTEXTO Y CRITERIOS	6
PROCESO DE EVALUACIÓN DE RIESGOS.....	9
IDENTIFICACIÓN DE RIESGOS.....	10
ANÁLISIS DE RIESGOS	13
EVALUACIÓN DE RIESGOS	18
TRATAMIENTO DE RIESGOS.....	21
PLANIFICACIÓN E IMPLEMENTACIÓN DE ACCIONES PARA EL TRATAMIENTO DE LOS RIESGOS	22
SEGUIMIENTOS Y REVISIONES	23
REGISTROS E INFORMES	23
OBLIGATORIEDAD	24
OFICIALIZACIÓN Y ACTUALIZACIÓN	24
VERSIONES ANTERIORES	24
CONTROL DE CAMBIOS	24
VIGENCIA	24
ANEXO	25
MATRIZ DE RIESGOS INSTITUCIONAL.....	25



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
	Manual de Gestión de Riesgos Institucional	Versión:	02
		Fecha de emisión:	27/11/2024
			Página 3 de 25

SIGLAS Y ABREVIATURAS

ISO: Organización Internacional de Normalización (Organization for Standardization).

INTRODUCCIÓN

Gestionar los riesgos es imprescindible para asegurar el éxito de la operatividad institucional, ya que ello implica abordar las incertidumbres que podrían afectar el logro de los objetivos de forma proactiva con la finalidad de minimizar las amenazas, maximizar las oportunidades y optimizar el logro de los objetivos institucionales.

Con el presente Manual de Gestión de Riesgos, el Instituto Administrador de los Beneficios de los Veteranos y Excombatientes adopta una cultura proactiva ante la gestión de riesgos, que facilite proceder de forma activa y consciente ante escenarios inciertos, desarrollando las mejores prácticas y procedimientos en las diferentes unidades organizativas, monitoreando y evaluando constantemente nuestra capacidad para identificar y gestionar el riesgo oportunamente y generando al mismo tiempo un modelo de gestión estructurado y en constante retroalimentación y mejora.

Este manual busca promover una cultura de gestión de riesgos en toda la institución, donde todas las personas empleadas del INABVE sean conscientes de los riesgos y participen activamente en la gestión de estos. Al mismo tiempo tiene como objetivo proporcionar un marco regulatorio integral para identificar, evaluar, mitigar y monitorear los riesgos que pueden afectar el logro de los objetivos institucionales.

OBJETIVOS

OBJETIVO GENERAL

Establecer un proceso sistemático para que cada área organizativa pueda anticipar, prevenir y responder a los riesgos, con el fin de minimizar el impacto negativo en la institución y aprovechar las oportunidades que surgen de una gestión proactiva de estos.

OBJETIVOS ESPECIFICOS

- Integrar la gestión de riesgos en todos los aspectos de la organización, desde el proceso de planificación hasta la ejecución operativa.
- Identificar y evaluar los riesgos permitiendo una comprensión más precisa de su probabilidad y consecuencia.
- Garantizar la transparencia, la responsabilidad y la participación de todos los empleados en la gestión de riesgos.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
Manual de Gestión de Riesgos Institucional		Fecha de emisión:	27/11/2024
		Página 4 de 25	

TERMINOLOGÍA

Administración/gestión de Riesgos: Es el conjunto de procesos, procedimientos y acciones que se implementan para identificar, medir, monitorear, controlar, informar y revelar los distintos tipos de riesgos a los que se encuentra expuesta una institución/empresa, de tal forma que les permita minimizar pérdidas y maximizar oportunidades.

Amenaza: Se define como la causa de un riesgo. La materialización de una amenaza dentro de un sistema organizacional puede originar uno o más riesgos.

Consecuencias: Se refiere a los resultados o impactos que pueden surgir de la ocurrencia de un evento de riesgo.

Cultura de gestión de riesgo: Es el conjunto de valores, actitudes y prácticas compartidas que caracterizan cómo una organización considera y enfrenta los riesgos de sus actividades.

Evento: Incidente o situación, que ocurre en un lugar determinado durante un período determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

Frecuencia: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del Riesgo: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Institución, que ponen en riesgo el logro de su Misión y objetivos.

Impacto: Se refiere a las consecuencias que podrían resultar de la materialización de un riesgo particular dentro de una organización o en un entorno específico.

Probabilidad: Se refiere a la posibilidad de ocurrencia de un riesgo potencial.

Riesgos Residuales: Nivel resultante del riesgo después de aplicar los controles.

Riesgo: La exposición a la posibilidad de ocurrencia de eventos que pueden impactar *negativamente en el logro de los objetivos institucionales*. Según la norma ISO 37001, es el efecto de la incertidumbre en los objetivos.

Soborno: Según la norma ISO 37001, es la oferta, promesa, entrega, aceptación o solicitud *de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera)*, directa o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
Página 5 de 25			

ALCANCE

Este manual comprende los procesos de identificación, evaluación y seguimiento de los riesgos operativos institucionales, excluyendo los tipos de riesgos gestionados por sistemas o normas específicas.

CAMPO DE APLICACIÓN

El Manual de Gestión de Riesgos es de aplicabilidad a todas las áreas organizativas del INABVE para identificar, evaluar y dar seguimiento a los riesgos que pudiesen obstaculizar o impedir el cumplimiento de los objetivos y metas institucionales.

NORMATIVA INTERNA

El presente manual se fundamenta en la siguiente normativa interna:

- Política de Revisión de Documentos.
- Instructivo para Aprobación de Documentos Institucionales.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
Manual de Gestión de Riesgos Institucional		Fecha de emisión:	27/11/2024
		Página 6 de 25	

GESTIÓN DE RIESGOS

FUNCIONES Y RESPONSABILIDADES PARA LA GESTIÓN DE RIESGOS

Para la ejecución de las actividades que requiere la gestión de riesgos, las áreas organizativas del INABVE tienen las siguientes responsabilidades:

Junta Directiva/Presidencia:

- Aprobación de recursos que guíen la identificación, evaluación y mitigación de riesgos.
- Dar por recibido informe de gestión de riesgos institucionales.

Gerencia General:

- Promover la gestión de riesgos en toda la institución.
- Asignar los recursos necesarios y pertinentes para la gestión de riesgos.
- Revisión de Informes sobre la gestión de riesgos presentados por las áreas competentes.

Jefaturas:

- Identificar y evaluar los riesgos de cada uno de sus procesos.
- Proponer las actividades de control para gestionar los riesgos identificados.
- Implementar acciones de control y seguimiento de los riesgos juntamente con las personas empleadas bajo su cargo.

Dirección de Planificación:

- *Colaborar y coordinar con todas las unidades organizativas en la identificación y elaboración de la matriz de riesgos.*
- Informar anualmente a las autoridades sobre la gestión de riesgos que afectan a la institución, así como el avance de los planes de acción de cada una de las áreas organizativas.

CONTEXTO Y CRITERIOS

CONTEXTO

La comprensión del contexto es importante porque:

- La gestión de riesgos tiene lugar en el contexto de los objetivos y las actividades de las organizaciones.
- Los factores organizacionales pueden ser una fuente de riesgos.
- El propósito y alcance del proceso de la gestión de riesgos puede estar interrelacionado con los objetivos de la organización como un todo.

Todas las instituciones públicas están sujetas a riesgos determinados por factores tanto externos como internos.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
	Manual de Gestión de Riesgos Institucional	Versión:	02
		Fecha de emisión:	27/11/2024
Página 7 de 25			

Factores Externos

Son aquellos que afectan la esencia misma de las instituciones, y provienen del entorno social, cultural, económico, político y legal. El análisis del contexto externo de las instituciones puede incluir, pero no limitarse a:

- Los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local.
- Modificaciones en las políticas y normativas establecidas por el gobierno central.
- Cambios en la jurisprudencia que pueden impactar las funciones específicas de una institución pública en un momento dado.
- Reformas y recortes presupuestarios que limitan la capacidad de gestión.
- Reducción o eliminación del presupuesto de inversión, lo que representa un riesgo significativo al impedir el cumplimiento de los objetivos institucionales.
- Las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas
- La complejidad de las redes y dependencias

Factores Internos

Son aquellos que se originan dentro de las instituciones y pueden, en un momento determinado, afectar la consecución de su misión y objetivos. El análisis del contexto interno de las instituciones puede incluir, pero no limitarse a:

- La visión, la misión y los valores.
- La estructura de las organizaciones, los roles y la rendición de cuentas.
- Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías).
- Las normas, las directrices y los modelos adoptados por las organizaciones.
- Las interdependencias e interconexiones.
- Los controles, procesos y procedimientos existentes.
- La disponibilidad del presupuesto.
- La gestión de los recursos humanos, materiales y financieros.
- Los intereses de las autoridades superiores.
- El nivel de motivación del personal.
- La manera en que se integran las personas a la institución.
- Los niveles salariales, entre otros.

Por ello, es necesario identificar los riesgos administrativos y operativos a los que está expuesto el INABVE, así como analizar, evaluar e implementar un plan para su adecuado manejo.

CRITERIOS

Cada unidad organizativa debe precisar la cantidad y el tipo de riesgos que puede o no tomar, con relación a los objetivos. También debe definir los criterios para evaluar la importancia de los riesgos y apoyar los procesos de toma de decisiones. Los criterios para riesgos se deben alinear con el marco de referencia de la administración/gestión de riesgos y adaptar al propósito y al alcance específicos de la actividad considerada. Los criterios para riesgos debieran reflejar los valores, objetivos y recursos de la institución coherentes con las políticas y declaraciones acerca de la administración/gestión de riesgos.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
	Manual de Gestión de Riesgos Institucional	Versión:	02
Fecha de emisión:		27/11/2024	
Página 8 de 25			

Los criterios se debieran definir teniendo en consideración las obligaciones de la institución y los puntos de vista de sus partes interesadas.

Aunque los criterios para riesgos se debieran establecer al principio del proceso de la evaluación de riesgos, éstos son dinámicos, y debieran revisarse continuamente y si fuese necesario, modificarse.

Para establecer los criterios para riesgos, se debiera considerar lo siguiente:

- La naturaleza y los tipos de incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles).
- Cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad.
- Los factores relacionados con el tiempo.
- La coherencia en el uso de las mediciones.
- Cómo se va a determinar el nivel de riesgos.
- Cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos.
- La capacidad de la organización misma.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
Manual de Gestión de Riesgos Institucional		Fecha de emisión:	27/11/2024
		Página 10 de 25	

IDENTIFICACIÓN DE RIESGOS

El propósito de la identificación es que cada área organizativa pueda detectar, reconocer y detallar los riesgos relevantes que puedan facilitar o dificultar el cumplimiento de los objetivos institucionales. Es esencial disponer de información adecuada y actualizada para llevar a cabo este proceso de identificación de manera efectiva.

En esta fase, las unidades organizativas deberán identificar los riesgos que podrían comprometer el cumplimiento de las actividades claves relacionadas con el cumplimiento de los objetivos del área, así como aquellas incluidas en sus respectivos Planes Operativos Anuales, ya que la materialización de estos conllevaría a que el alcance de los resultados esperados y los objetivos operativos y/o estratégicos planteados puedan verse afectados.

Factores de riesgo

Las áreas organizativas pueden utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se debieran considerar los factores siguientes y la relación entre estos:

- Las fuentes de riesgos tangibles e intangibles.
- Las causas y los eventos.
- Las amenazas y las oportunidades.
- Las vulnerabilidades y las capacidades.
- Los cambios en los contextos interno y externo.
- Los indicadores de riesgos emergentes.
- La naturaleza y el valor de los activos y los recursos.
- Las consecuencias y sus impactos en los objetivos.
- Las limitaciones de conocimiento y la confiabilidad de la información.
- Los factores relacionados con el tiempo.
- Los sesgos, los supuestos y las creencias de las personas involucradas.

Tipos de riesgos

Las categorías en las que se pueden clasificar los riesgos que enfrenta la institución son los siguientes:

Riesgo de Corrupción: Se asocian a la posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad para la obtención de un beneficio en particular.

Riesgo de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la población.

Riesgo de Imagen (Reputacional): Resultará cuando la credibilidad del INABVE este en tela de juicio por acontecimientos dados a conocer al público.

Riesgo de Soborno: Se refiere a la probabilidad de que se presenten situaciones en las que una persona o entidad ofrezca, entregue o reciba un soborno para influir en decisiones o acciones.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 11 de 25	

Riesgo Estratégico: Incluye los obstáculos externos o internos que no le permitirán al INABVE el cumplir sus objetivos. Están asociados además con la planificación estratégica y operativa, gestión del talento humano, la gestión del seguimiento de la entrega de beneficios y la forma en que se administra la entidad.

Riesgo Financiero: Se relacionan con el manejo de los recursos financieros de la Institución que incluye, la gestión de los ingresos, la formulación del presupuesto, el manejo del efectivo, los registros de los hechos económicos, registros de la ejecución financiera, la generación de los estados financieros, los pagos a proveedores y la gestión administrativa de bienes y servicios.

Riesgo Operativo: Comprende los riesgos relacionados tanto con la parte operativa como técnica de la Institución, incluye riesgos provenientes en los sistemas de información, seguimiento a la ejecución física de la entrega de beneficios, en la definición de los procesos, en la estructura de la entidad.

Riesgo Político: Son las acciones de un gobierno transformadas por medio de decisiones del sistema judicial, nuevas leyes, decretos presidenciales, o acontecimientos independientes, tales como: Guerras, tumultos, disturbios sociales, entre otros.

Riesgo Tecnológico: Se asocian con el tema de tecnología en el ámbito de informática, así como también en lo relacionado a la seguridad de los sistemas y/o aplicaciones informáticas, correos electrónicos, sistemas de información, pérdida o robo de equipos, etc.; y además con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras, respaldando el cumplimiento de la misión.



Ilustración 1. Matriz para identificación de riesgos.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO

Ilustración 2. Ejemplo de identificación de riesgos.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO
1	DJUD	Riesgo de cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.
2	RRHH	Riesgo operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.
3	TICS	Riesgo tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos
4	GFIN	Riesgo Financiero	Riesgo de fraude interno, como malversación de fondos o falsificación de documentos.
5	UGDA	Riesgo operativo	Riesgo de pérdida o mal manejo de documentos legales y registros



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 13 de 25	

ANÁLISIS DE RIESGOS

Este análisis suministra información para evaluar los riesgos, tomar decisiones respecto a cómo abordarlos, determinar si es necesario hacerlo y seleccionar las estrategias y enfoques más adecuados para tratarlos. Los resultados del análisis ofrecen una comprensión detallada para la toma de decisiones cuando se enfrentan diferentes alternativas, y estas opciones conllevan distintos tipos y niveles de riesgo.

Una vez que todas las áreas organizativas hayan identificado los principales riesgos estratégicos, administrativos y operativos que afectan su labor, deberán analizarlos objetivamente con el propósito de conocer el grado en que estos afectan el logro de los objetivos planteados.

El análisis debe considerar factores tales como:

- La probabilidad de los eventos y de las consecuencias.
- La naturaleza y la magnitud de las consecuencias.
- La complejidad y la interconexión.
- Los factores relacionados con el tiempo y la volatilidad.
- La efectividad de los controles existentes.
- Los niveles de sensibilidad y de confianza.

El método de análisis cuantitativo de riesgos implica la asignación de valores numéricos a la probabilidad y al impacto de los riesgos, lo que permite calcular métricas como el valor del riesgo. El análisis cuantitativo de riesgos se basa en datos y modelos matemáticos para evaluar la exposición al riesgo y la efectividad de las estrategias de mitigación.

Probabilidad

Se refiere a la posibilidad de que ocurra un evento o situación que pueda afectar los objetivos de un área organizativa y en consecuencia los objetivos de la institución. Es una medida de la frecuencia con la que se espera que un riesgo específico ocurra en un periodo de tiempo determinado. La probabilidad es una parte fundamental del análisis de riesgos, ya que, junto con el impacto, ayuda a determinar la importancia y prioridad de los riesgos identificados.



Ilustración 3. Criterios para estimar probabilidad.

	Nivel	Tipo de probabilidad	Descriptivo	Rango de probabilidad	Escala de ocurrencia
PROBABILIDAD	3	Alta	Ocurrirá en la mayoría de las circunstancias.	Probabilidad por arriba del 80% de que este se presente.	Ocurre todas las semanas
	2	Media	Puede ocurrir en algún momento.	Entre el 40% y el 80% de probabilidad que este se presente.	Ocurre cada mes
	1	Baja	Puede ocurrir en circunstancias excepcionales	Entre el 1% y el 40% de probabilidad que este se presente.	Ocurre dos veces al año



Ilustración 4. Ejemplo de estimación de probabilidad.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO	PROBILIDAD DE OCURRENCIA	
1	DJUD	Riesgo de Cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.	Media	2
2	RRHH	Riesgo Operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.	Alta	3
3	TICS	Riesgo Tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos	Baja	1
4	GFIN	Riesgo Financiero	Riesgo de fraude interno, como malversación de fondos o falsificación de documentos.	Baja	1
5	UGDA	Riesgo Operativo	Riesgo de pérdida o mal manejo de documentos legales y registros	Media	2

Consecuencias

Son los efectos no deseados o adversos que pueden surgir si un riesgo se materializa. Pueden incluir pérdidas financieras, daño a la reputación, interrupción de operaciones, lesiones a personas, daño al medio ambiente, entre otros. La gestión de riesgos busca identificar, evaluar y mitigar estos riesgos para minimizar su impacto negativo.



Ilustración 5. Criterios para estimar consecuencias.

	Nivel	Tipo de consecuencia	Pérdidas económicas	Afectación al patrimonio	Legal y cumplimiento	Afectación de la operación	Reputacional
CONSECUENCIA	3	Alta	Pérdidas económicas de alto impacto > 15% del presupuesto asignado. Pérdidas económicas críticas que ponen en peligro la estabilidad financiera de la institución, su capacidad para operar, la prestación de servicios esenciales y el cumplimiento de objetivos.	Daños o pérdidas críticas que ponen en peligro la integridad del patrimonio y la capacidad operativa de la institución. Este nivel de afectación es grave y puede comprometer el funcionamiento a largo plazo.	Impacto crítico con consecuencias legales muy graves, incluyendo litigios de alto perfil, sanciones severas, o multas altas; estos pueden afectar gravemente la reputación y estabilidad de la institución, además de causar un impacto financiero significativo.	Mayor a 21 días	Revelaciones masivas que causan un daño irreparable a la reputación.
	2	Media	Pérdidas económicas moderadas 5% y <15% del presupuesto asignado. Pérdidas económicas que generan un impacto considerable, que requieren revisiones sustanciales del presupuesto y posibles retrasos o modificaciones en proyectos o servicios.	Daños o pérdidas significativas que requieren intervenciones sustanciales para ser gestionados y que afectan la capacidad operativa o financiera de la institución, aunque sin poner en peligro la continuidad total.	Impacto significativo con consecuencias legales significativas, que pueden incluir multas moderadas, sanciones, o cambios obligatorios en procedimientos. Involucra acciones legales que, aunque sean importantes, no ponen en peligro la operación total de la institución, pero requieren cambios estructurales o ajustes sustanciales.	15 días	Revelaciones que dañan seriamente la reputación y generan preocupación pública.
	1	Baja	Pérdidas económicas bajas < 5% del presupuesto asignado. Pérdidas económicas relativamente pequeñas y manejables, con un impacto limitado en las operaciones generales de la institución.	Daños que no afectan gravemente el patrimonio ni la capacidad operativa. Son manejables con reparaciones o reposiciones menores sin un impacto significativo en la operación general.	Impacto bajo relacionado con problemas de cumplimiento menores. Las consecuencias legales son manejables y puede requerir acciones correctivas limitadas, como ajustes menores en contratos o procedimientos, se puede corregir con acciones correctivas menores.	5 días	Acusaciones con alguna evidencia pero sin consecuencias graves.



Ilustración 6. Ejemplo de estimación de consecuencias.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO	PROBILIDAD DE OCURRENCIA		CONSECUENCIA	
1	DJUD	Riesgo de Cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.	Media	2	Media	2
2	RRHH	Riesgo Operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.	Alta	3	Alta	3
3	TICS	Riesgo Tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos	Baja	1	Alta	3
4	GFIN	Riesgo Financiero	Riesgo de fraude interno, como malversación de fondos o falsificación de documentos.	Baja	1	Baja	1
5	UGDA	Riesgo Operativo	Riesgo de pérdida o mal manejo de documentos legales y registros	Media	2	Baja	1

Valor inicial del riesgo

En esta etapa se valorará la probabilidad de ocurrencia del riesgo y el impacto que puede producirse en caso de que se materialice para la valorización de los riesgos es importante considerar los factores de los riesgos (causas) sus resultados, sus efectos y la probabilidad de que riesgos se materialicen y, por tanto, ocurran los resultados o impactos identificados.

Ilustración 7. Valoración de riesgos.

		VALOR DEL RIESGO			
PROBABILIDAD	ALTA	3	MODERADO	ALTO	EXTREMO
			3	6	9
	MEDIA	2	BAJO	ALTO	ALTO
			2	4	6
	BAJA	1	BAJO	BAJO	MODERADO
			1	2	3
			1	2	3
			BAJA	MEDIA	ALTA
			CONSECUENCIA		



Ilustración 8. Ejemplo de valoración de riesgos.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO	PROBILIDAD DE OCURRENCIA		CONSECUENCIA		VALORACIÓN DEL RIESGO	
1	DJUD	Riesgo de Cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.	Media	2	Media	2	Alto	4
2	RRHH	Riesgo Operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.	Alta	3	Alta	3	Extremo	9
3	TICS	Riesgo Tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos	Baja	1	Alta	3	Moderado	3
4	GFIN	Riesgo Financiero	Riesgo de fraude interno, como malversación de fondos o falsificación de documentos.	Baja	1	Baja	1	Bajo	1
5	UGDA	Riesgo Operativo	Riesgo de pérdida o mal manejo de documentos legales y registros	Media	2	Baja	1	Bajo	2

EVALUACIÓN DE RIESGOS

El propósito de la evaluación de los riesgos es apoyar a la toma de decisiones. La evaluación de los riesgos implica comparar los resultados del análisis del riesgo con los criterios para riesgos establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

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

Las decisiones debieran tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas internas y externas.



Ilustración 9. Evaluación de riesgos.

Valor de riesgo	Rango de valor del riesgo	Evaluación del riesgo
Extremo	9	MITIGAR. Puede causar daños significativos e irreparables al Instituto. Se deben diseñar e implementar planes de acción que reduzcan tanto la probabilidad como el impacto del riesgo. Esto incluye la asignación de recursos y el establecimiento de plazos claros para las acciones.
Alto	de 4 a 6	INVESTIGAR. Puede tener consecuencias serias que afectan la operación y los objetivos de la organización. Se requiere un análisis profundo para comprender el riesgo y desarrollar planes de acción preventivos que minimicen su probabilidad o impacto.
Moderado	3	MANTENER. Puede tener consecuencias notables, pero son administrables. Se deben establecer controles rutinarios y medidas de monitoreo continuo para mantener el riesgo bajo supervisión y activar planes de contingencia si es necesario.
Bajo	de 1 a 2	ASUMIR. No representa una amenaza significativa. Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo. Aunque no se requieren controles estrictos, es recomendable tener protocolos listos para una rápida adaptación si la situación cambia.



Ilustración 10. Ejemplo de evaluación de riesgos.

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO	PROBILIDAD DE OCURRENCIA		CONSECUENCIA		VALORACIÓN DEL RIESGO	EVALUACIÓN DEL RIESGO	
1	DJUD	Riesgo de Cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.	Media	2	Media	2	Alto	4	INVESTIGAR: Se requiere un análisis profundo para comprender el riesgo y desarrollar planes de acción preventivos que minimicen su probabilidad o impacto.
2	RRHH	Riesgo Operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.	Alta	3	Alta	3	Extremo	9	MITIGAR: Se deben diseñar e implementar planes de acción que reduzcan tanto la probabilidad como el impacto del riesgo. Esto incluye la asignación de recursos y el establecimiento de plazos claros para las acciones.
3	TICS	Riesgo Tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos	Baja	1	Alta	3	Moderado	3	MANTENER: Se deben establecer controles rutinarios y medidas de monitoreo continuo.
4	GFIN	Riesgo Financiero	Riesgo de fraude interno, como malversación de fondos o falsificación de documentos.	Baja	1	Baja	1	Bajo	1	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.
5	UGDA	Riesgo Operativo	Riesgo de pérdida o mal manejo de documentos legales y registros	Media	2	Baja	1	Bajo	2	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 21 de 25	

TRATAMIENTO DE RIESGOS

El propósito del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos. El tratamiento de los riesgos implica un proceso iterativo de:

1. Formular y seleccionar opciones para el tratamiento de los riesgos.
2. Planear e implementar el tratamiento de los riesgos.
3. Evaluar la efectividad de dicho tratamiento.
4. Decidir si los riesgos residuales son aceptables o si requiere efectuar algún tratamiento adicional.

SELECCIÓN DE LAS OPCIONES PARA TRATAMIENTO DE RIESGOS

La selección de las opciones más apropiadas para el tratamiento de riesgos implica para cada área organizativa hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación. Las opciones de tratamiento de los riesgos no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar los riesgos pueden implicar una o más de las siguientes:

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo mismo.
- Aceptar o aumentar el riesgo en busca de una oportunidad.
- Eliminar la fuente de riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);
- Retener el riesgo con base en una decisión informada.

La elección de cómo tratar los riesgos debería estar en línea con los objetivos institucionales, los criterios de riesgo y los recursos disponibles. Al considerar opciones para el tratamiento de riesgos, la institución debe tener en cuenta los valores, percepciones y la posible participación de las partes interesadas, así como los medios adecuados para comunicarse y consultar con ellos.



PLANIFICACIÓN E IMPLEMENTACIÓN DE ACCIONES PARA EL TRATAMIENTO DE LOS RIESGOS

El propósito de los planes para el tratamiento de los riesgos es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planeado. El plan de tratamiento debiera identificar claramente el orden en el cual el tratamiento del riesgo se debiera implementar.

Ilustración 11. Acciones para tratamiento de riesgos.

VALORACIÓN DEL RIESGO		EVALUACIÓN DEL RIESGO	ACCIONES	RESPONSABLES	FECHAS DE LAS ACCIONES
Alto	4	INVESTIGAR: Se requiere un análisis profundo para comprender el riesgo y desarrollar planes de acción preventivos que minimicen su probabilidad o impacto.			
Extremo	9	MITIGAR: Se deben diseñar e implementar planes de acción que reduzcan tanto la probabilidad como el impacto del riesgo. Esto incluye la asignación de recursos y el establecimiento de plazos claros para las acciones.			
Moderado	3	MANTENER: Se deben establecer controles rutinarios y medidas de monitoreo continuo.			
Bajo	1	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.			
Bajo	2	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.			

EVALUAR LA EFECTIVIDAD DEL TRATAMIENTO DE LOS RIESGOS

El tratamiento de riesgos puede generar nuevos riesgos que también necesitan ser gestionados. Si no hay opciones disponibles para tratar un riesgo o si las opciones existentes no reducen adecuadamente los riesgos, esto debe ser registrado y revisado regularmente.

Ilustración 11. Evaluación de efectividad del tratamiento de riesgos.

VALORACIÓN DEL RIESGO		EVALUACIÓN DEL RIESGO	ACCIONES	RESPONSABLES	FECHAS DE LAS ACCIONES	ESTADO DE LAS ACCIONES REALIZADAS	NUEVA PROBABILIDAD	NUEVA CONSECUENCIA	VALORACIÓN DEL RIESGO RESIDUAL
Alto	4	INVESTIGAR: Se requiere un análisis profundo para comprender el riesgo y desarrollar planes de acción preventivos que minimicen su probabilidad o impacto.					Baja 1	Baja 1	BAJO 1
Extremo	9	MITIGAR: Se deben diseñar e implementar planes de acción que reduzcan tanto la probabilidad como el impacto del riesgo. Esto incluye la asignación de recursos y el establecimiento de plazos claros para las acciones.					Baja 1	Baja 1	BAJO 1
Moderado	3	MANTENER: Se deben establecer controles rutinarios y medidas de monitoreo continuo.					Baja 1	Baja 1	BAJO 1
Bajo	1	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.					Baja 1	Baja 1	BAJO 1
Bajo	2	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.					Baja 1	Baja 1	BAJO 1



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 23 de 25	

DECIDIR SI LOS RIESGOS RESIDUALES SON ACEPTABLES O SI REQUIERE EFECTUAR ALGÚN TRATAMIENTO ADICIONAL

Las personas responsables de tomar decisiones y otras partes interesadas deben estar informadas sobre la naturaleza y el nivel de los riesgos residuales después de que un riesgo haya sido tratado. Estos riesgos residuales deben ser documentados y monitoreados, revisados y, si es necesario, tratados adicionalmente.

SEGUIMIENTOS Y REVISIONES

El objetivo del seguimiento y las revisiones de las acciones es garantizar y mejorar la calidad y efectividad del diseño, la implementación y los resultados del proceso. Es crucial que el seguimiento continuo y la revisión periódica del proceso de gestión de riesgos y sus resultados sean una parte planificada e integral de dicho proceso, con responsabilidades claramente definidas.

El seguimiento y revisiones evalúa la efectividad de los planes de acción implementados, la evolución de los niveles de riesgo de un periodo a otro, la persistencia de riesgos significativos y los riesgos inaceptables, así como la efectividad de los controles.

REGISTROS E INFORMES

El proceso de la administración/gestión de riesgos y sus resultados se debieran documentar e informar a través de los mecanismos apropiados. Los registros y reportes pretenden:

- Comunicar las actividades de la administración/gestión de riesgos y sus resultados a nivel institucional.
- Ofrecer información para la toma de decisiones.
- Mejorar las actividades de la administración/gestión de riesgos.
- Apoyar en la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la administración/gestión de riesgos.

Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada debieran tener en cuenta, pero no limitarse su uso, la sensibilidad de la información y los contextos interno y externo.

La Dirección de Planificación realizará anualmente un proceso de consolidación de documentación referente a las matrices de riesgos elaboradas por las áreas organizativas y las acciones implementadas. El informe resultante de este proceso será entregado a las autoridades del instituto, proporcionando con ello una base sólida para la toma de decisiones estratégicas y la asignación de recursos para la gestión de riesgos a futuro.



	Instituto Administrador de los Beneficios de los Veteranos y Excombatientes	Código:	MNL-INST-0003.2
		Versión:	02
	Manual de Gestión de Riesgos Institucional	Fecha de emisión:	27/11/2024
		Página 24 de 25	

OBLIGATORIEDAD

El presente manual es de obligatoria aplicación para todas las áreas organizativas como responsables de los procesos administrativos, financieros y operativos que se desarrollan en el INBVE.

OFICIALIZACIÓN Y ACTUALIZACIÓN

Para su aprobación y difusión el presente manual deberá cumplir lo establecido en el **Instructivo para Aprobación de Documentos**; asimismo, para su actualización o modificación se deberá seguir lo determinado en la **Política de Revisión de Documentos**.

VERSIONES ANTERIORES

Cualquier versión anterior de este documento será automáticamente sustituida por esta nueva versión a partir de la fecha de su aprobación por Junta Directiva. La nueva versión reemplaza todas las disposiciones, términos y condiciones establecidos en la versión previa.

CONTROL DE CAMBIOS

Codificación	Versión	Fecha	Motivo del cambio
MNL-INST-0003.1	1	18/05/23	Versión inicial del documento.
MNL-INST-0003.2	2	27/11/24	<ul style="list-style-type: none"> Enfoque del documento a la norma ISO 37001. Actualización de formato de matriz de riesgos, escalas de probabilidad, consecuencia y valor de riesgo.

VIGENCIA

El presente manual entrará en vigencia posterior a su aprobación por Junta Directiva.





ANEXO

MATRIZ DE RIESGOS INSTITUCIONAL

N°	AREA	TIPO DE RIESGO	RIESGO IDENTIFICADO	PROBILIDAD DE OCURRENCIA	CONSECUENCIA	VALORACIÓN DEL RIESGO	EVALUACIÓN DEL RIESGO	ACCIONES	RESPONSABLES	FECHAS DE LAS ACCIONES	ESTADO DE LAS ACCIONES REALIZADAS	NUEVA PROBABILIDAD	NUEVA CONSECUENCIA	VALORACIÓN DEL RIESGO RESIDUAL	OBSERVACIONES DE LA IMPLEMENTACIÓN
1	DJJD	Riesgo de Cumplimiento	Riesgo de multas y sanciones regulatorias debido al incumplimiento de normativas o leyes gubernamentales.	Media 2	Media 2	Alto 4	INVESTIGAR: Se requiere un análisis profundo para comprender el riesgo y desarrollar planes de acción preventivos que minimicen su probabilidad e impacto.					Baja 1	Baja 1	BAJO 1	
2	RRRH	Riesgo Operativo	Riesgo de pérdida de conocimiento y experiencia debido a una alta rotación de personal en puestos críticos.	Alta 3	Alta 3	Extremo 9	MITIGAR: Se deben diseñar e implementar planes de acción que reduzcan tanto la probabilidad como el impacto del riesgo. Esto incluye la asignación de recursos y el establecimiento de plazos claros para las acciones.					Baja 1	Baja 1	BAJO 1	
3	TICS	Riesgo Tecnológico	Riesgo de ataques informáticos, como malware, ransomware o phishing, que pueden comprometer la integridad y confidencialidad de los datos.	Baja 1	Alta 3	Moderado 3	MANTENER: Se deben establecer controles rutinarios y medidas de monitoreo continuo.					Baja 1	Baja 1	BAJO 1	
4	QFIN	Riesgo Financiero	Riesgo de fraudes internos, como malversación de fondos o falsificación de documentos.	Baja 1	Baja 1	Bajo 1	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.					Baja 1	Baja 1	BAJO 1	
5	UGDA	Riesgo Operativo	Riesgo de pérdida o mal manejo de documentos legales y registros.	Media 2	Baja 1	Bajo 2	ASUMIR: Se deben implementar políticas de monitoreo que permitan un seguimiento del riesgo.					Baja 1	Baja 1	BAJO 1	

