



PERÚ

Ministerio de  
Educación

Instituto Peruano  
del Deporte

"Año del Buen Servicio al Ciudadano"

## Resolución de Presidencia N° 279-2017-IPD/P.....

Lima 24 de Noviembre del 2017.....

**VISTO:** El Memorando N°4376-2017-IPD/OPP de fecha 10 de noviembre 2017 y el Informe N° 818-2017-IPD/OAJ, de fecha 22 de noviembre 2017;

### CONSIDERANDO:

Que, el Instituto Peruano del Deporte, en adelante IPD, conforme a la Ley N° 28036, Ley de Promoción y Desarrollo del Deporte, es el órgano rector del Sistema Deportivo Nacional, constituye un organismo público ejecutor y cuenta con autonomía funcional, administrativa y presupuestal;

Que, mediante Resolución de Contraloría N° 004-2017-CG, se aprueba la Guía para la implementación y fortalecimiento del Sistema de control Interno en la Entidades del Estado;

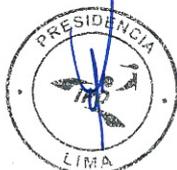
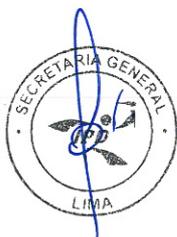
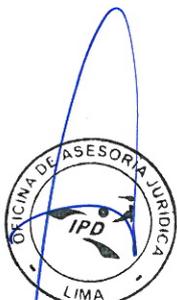
Que, la Guía precitada, tiene como finalidad el fortalecer el Control Interno para el eficiente, transparente y adecuado ejercicio de la función pública en el uso de los recursos del Estado;

Que, en la etapa II, la acotada Guía establece la identificación de brechas, donde se determina el estado situacional actual del Sistema de Control Interno (SCI) dentro de la Entidad, constituyendo dicha información, el insumo principal para la implementación del referido Sistema de Control, debiéndose efectuar un análisis de la gestión de riesgos de la entidad, requiriéndose contar con una política de riesgos, metodología y plan de gestión de riesgos, de conformidad con el Anexo N° 13 de dicha Guía;

Que, en virtud de lo señalado precedentemente, la Secretaría General formula el proyecto de Manual denominado "Manual de gestión de riesgos del Instituto Peruano del Deporte";

Que, dicho documento tiene por finalidad establecer la metodología y procedimientos que permiten al IPD, realizar una adecuada administración de riesgos, metodología y plan de gestión de riesgos;

Que, a través del Informe N° 818-2017-IPD/OAJ, la Oficina de Asesoría Jurídica señala que el Manual descrito precedentemente, cumple con los lineamientos contenidos en la Resolución de Contraloría N° 004-2017-CG, que aprueba la Guía para la implementación y fortalecimiento del Sistema de Control Interno en las entidades del Estado y no contraviene ninguna norma del ordenamiento legal vigente, por lo que resulta viable su aprobación;





PERÚ

Ministerio de  
Educación

Instituto Peruano  
del Deporte

"Año del Buen Servicio al Ciudadano"

De conformidad con lo dispuesto en la Ley N° 28036 – Ley de Promoción y Desarrollo del Deporte y sus modificatorias, el Reglamento de la Ley de Promoción y Desarrollo del Deporte aprobado mediante Decreto Supremo N° 018-2004-PCM, el Reglamento de Organización y Funciones del Instituto Peruano del Deporte, aprobado mediante Decreto Supremo N° 017-2004-PCM y modificado por el Decreto Supremo N° 086-2004-PCM;

Con los vistos de la Secretaría General, de la Oficina de Presupuesto y Planificación y la Oficina de Asesoría Jurídica;

**SE RESUELVE:**

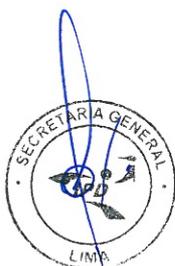
**Artículo 1.-** Aprobar el Manual de Gestión de Riesgos del Instituto Peruano del Deporte, que en anexo adjunto, forma parte integrante de la presente resolución.

**Artículo 2.-** Publicar el Manual de Gestión de Riesgos del Instituto Peruano del Deporte en la página web del Instituto Peruano del Deporte ([www.ipd.gob.pe](http://www.ipd.gob.pe)).

**Regístrese y comuníquese.**



  
.....  
OSCAR FERNÁNDEZ CÁCERES  
Presidente  
INSTITUTO PERUANO DEL DEPORTE





**MANUAL DE GESTION DE RIESGOS  
DEL INSTITUTO PERUANO DEL  
DEPORTE**

## ÍNDICE

1.	FINALIDAD.....	3
2.	OBJETIVO.....	3
3.	ALCANCE.....	3
4.	BASE LEGAL.....	3
5.	DEFINICIONES.....	3
6.	DISPOSICIONES GENERALES.....	4
7.	DISPOSICIONES ESPECÍFICAS.....	5
8.	DISPOSICIÓN COMPLEMENTARIA .....	13



## 1. FINALIDAD

Contar con un método sistemático para la administración de riesgos, identificando, analizando, valorando y dando respuesta a los riesgos a los que está expuesto el Instituto Peruano del Deporte, optimizando los recursos disponibles a través de la minimización de las pérdidas que pudieran presentarse como por la no consecución de sus objetivos.

## 2. OBJETIVO

Establecer la metodología y procedimientos que permitan al Instituto Peruano del Deporte, realizar una adecuada administración de riesgos.

## 3. ALCANCE

Las disposiciones contenidas en el presente instrumento son de estricto cumplimiento de los órganos y unidades orgánicas del IPD, así como de los funcionarios y servidores involucrados en cada uno de los procesos existentes.

## 4. BASE LEGAL

- Constitución Política del Perú.
- Ley 27785 - Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
- Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado y su modificatoria.
- Ley N° 28036 – Ley de Promoción y Desarrollo del Deporte, sus modificatorias y su Reglamento, aprobado mediante Decreto Supremo N° 018-2004-PCM.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2021.
- Decreto Supremo N° 017-2004-PCM que aprueba el Reglamento de Organización y Funciones del IPD.
- Resolución de Contraloría N° 149-2016-CG, que aprueba la Directiva N° 013-2016-CG/GPROD “Implementación del Sistema de Control Interno de las entidades del Estado”.
- Control Interno – Marco Integrado COSO 2013.
- Resolución de Contraloría N° 004-2017-CG que aprueba la “Guía para la Implementación y Fortalecimiento del Sistema de Control Interno en las Entidades del Estado”.

## 5. DEFINICIONES

### 5.1 Diagrama de Flujos o Procesos

Es una representación gráfica de la secuencia de actividades, dentro de un proceso o un procedimiento. Cada paso del proceso es representado por un símbolo diferente que contiene la descripción de la etapa del proceso.

### 5.2 Evaluación de riesgo

Es el análisis del riesgo que puede surgir de situaciones o acciones en un contexto determinado, teniendo en cuenta lo adecuado de los controles existentes y la aceptabilidad del riesgo.

### 5.3 Impacto

Son las consecuencias provocadas a la Entidad. El impacto de los eventos y el riesgo consecuente será evaluado desde el punto de vista inherente y residual.

### 5.4 Mapa de Procesos

Es un diagrama que representa, a manera de inventario gráfico, los procesos de una organización en forma interrelacionada.

**5.5 Probabilidad**

Es la posibilidad de que un evento potencial, identificado como riesgo, pueda convertirse en un evento real.

**5.6 Riesgo**

Es una situación, evento o condición futura que podría ocurrir o no, y que de ocurrir, afectaría la capacidad para cumplir con los objetivos de la Entidad, de los procesos o de los proyectos. Si la afectación es negativa, entonces se considera un riesgo, y si es positiva, una oportunidad. La gestión de un riesgo estará afectada por su probabilidad de ocurrencia.

**5.7 Riesgo Inherente**

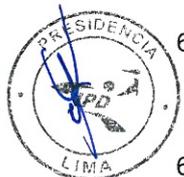
Es aquel que existe por la naturaleza de la prestación del servicio.

**5.8 Riesgo Residual**

Es aquel que permanece a pesar de haber aplicado las acciones de control necesarias para reducir la probabilidad y consecuencia del riesgo.

**6. DISPOSICIONES GENERALES**

6.1 La metodología para la administración de riesgos es aplicada a nivel de Entidad y a nivel de procesos, por lo que se requiere el análisis y entendimiento de los mismos. Para el primer caso, estará en función a los objetivos estratégicos institucionales establecidos en el PEI del IPD y el segundo, en función a los objetivos de cada proceso.



6.2 Esta metodología permite administrar los riesgos que pueden tener un impacto negativo en el logro de los objetivos institucionales para que, a través de la implementación de planes de acción, mantenga el nivel de riesgo dentro de la tolerancia aceptada por el IPD.

6.3 La metodología deberá ser aplicada por todas las dependencias, siendo el Comité de Riesgos del IPD, el encargado de apoyar y asistir al Comité de Control Interno en su aplicación.



6.4 Todos los órganos y unidades orgánicas del IPD evalúan el riesgo operacional de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el servicio a prestar, a fin de que se adopten las acciones necesarias para su mitigación.

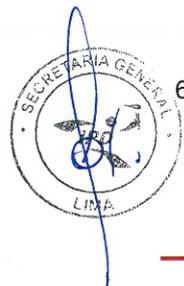
6.5 La metodología a desarrollar combina criterios cuantitativos y cualitativos para determinar el nivel de exposición al riesgo, y tiene las siguientes etapas: la identificación, evaluación, tratamiento, control, comunicación e información y monitoreo, de los riesgos.

6.6 Los órganos y unidades orgánicas responsables, garantizan que las contrataciones significativas o críticas sean adecuadamente administradas, de tal manera que cuando se produzca una falla o suspensión del objeto de contrato, se ejecuten oportunamente acciones de mitigación de sus riesgos.



6.7 El IPD implementa un Sistema de Gestión de la Seguridad de la Información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

6.8 Los órganos y unidades orgánicas, sobre los objetivos establecidos en el PEI y en el POI del IPD, identificarán los riesgos a razón de las amenazas y debilidades, debiendo llenar la información de su competencia de acuerdo al Plan de Gestión de Riesgos del IPD; para ello es importante conocer cuáles son los procesos en los que intervienen.



6.9 El Comité de Riesgos del IPD será el encargado de verificar la información remitida por los órganos y unidades orgánicas, a fin de priorizar los riesgos dentro del contexto estratégico del IPD. Dicho análisis deberá ser presentado mediante un informe sustentado con la

evaluación del costo – beneficio, el cual será dirigido a la Alta Dirección para su aprobación, previo conocimiento del Comité de Control Interno.

Dicho Comité deberá supervisar el cumplimiento de los cronogramas de atención que realicen los órganos o unidades orgánicas.

## 7. DISPOSICIONES ESPECÍFICAS

### 7.1 Componentes del proceso de gestión de riesgos

La gestión del riesgo en el IPD, considera la comprensión del contexto externo e interno, que implica identificar aquellos elementos que tendrían incidencia en el logro de los objetivos.

El contexto externo, incluye aspectos del entorno social y cultural, normativos, legales, financieros, tecnológicos, económicos, naturales, a nivel nacional, regional o local, factores y tendencias que afectan al cumplimiento de los objetivos institucionales, así como las relaciones con las partes interesadas externas (usuarios, proveedores, otras entidades del Estado, entre otros).

El contexto interno, comprende la administración interna, organización, funciones, responsabilidades, políticas, objetivos y estrategias para alcanzarlos, su cultura organizacional, sistemas de información (aplicativos), activos de información, flujo de información, procesos de toma de decisiones y comprensión de la gestión de riesgo por parte de todos los servidores y funcionarios.

Esta comprensión permite determinar el alcance que tendrán las siguientes etapas que comprenden el proceso de gestión de riesgos del IPD.

### 7.2 Identificación de riesgos

Consiste en la identificación de eventos (amenazas) potenciales de riesgo que afecten el logro de los objetivos de un proceso, así como las causas, vulnerabilidades y los factores que los originan.

Este proceso se encuentra a cargo de los órganos y unidades orgánicas a través de los servidores y funcionarios involucrados en cada uno de los procesos del IPD.

#### **Factores que originan riesgos**

Los riesgos operacionales pueden originarse debido a cuatro factores: personal, procesos internos, tecnología de información y eventos externos.

- **Personal:** Comprende la posibilidad de pérdidas relacionadas a negligencia, error humano, sabotaje, fraude interno, robo, incumplimiento intencional de normas, autorizaciones incorrectas, coimas, apropiación de información sensible, falta de especificaciones claras en los términos de contratación del personal, entre otros. También se incluyen las pérdidas asociadas a entrenamiento y capacitación inadecuada.
- **Procesos internos:** Relacionado con el diseño inapropiado de los procesos críticos, o con políticas o procedimientos inadecuados o inexistentes que puedan tener como

consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos. Podrían considerarse los riesgos asociados a las fallas en los modelos utilizados, evaluación inadecuada de contratos, demora en la realización de tareas, normas desactualizadas o inexistentes, cláusulas confusas, dualidad de funciones e incumplimiento de plazos.

- **Tecnología de la información:** Comprenden las fallas en la seguridad y continuidad operativa de los sistemas informáticos, errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, no adecuada inversión en tecnología. Se incluye también infidencia de datos, acceso a datos no autorizados, comunicaciones, falla en el hardware, falla en el software, falla en telecomunicaciones, no adecuada arquitectura de comunicaciones.
- **Evento externo:** Asociados a eventos externos ajenos al control del IPD, relacionados a fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y actos delictivos, fallas en los servicios críticos provistos por terceros, el cambio de leyes, regulaciones o guías, estafa por personas ajenas al IPD, no adecuado cumplimiento de obligaciones por parte de los proveedores.

### 7.3 Análisis de los riesgos

En esta etapa se mide la amplitud con que la potencial ocurrencia de los riesgos identificados impacta en los objetivos del proceso. La evaluación se realiza desde dos perspectivas: la probabilidad y el impacto. La primera de ellas representa la posibilidad que se materialice, mientras que la segunda refleja su efecto.

Para dicho fin, el IPD aplicará la Matriz de Calificación de Riesgos, la cual está formada por una cuadrícula con la probabilidad de ocurrencia en el eje vertical y el impacto en el eje horizontal, de tal forma que los riesgos se distribuyan en base a éstas dos variables. Un riesgo se considera importante cuando tiene una probabilidad o un impacto elevado, lo que permite delimitar diferentes áreas dentro de esta matriz. **(Tabla N° 01)**



**TABLA N° 01 MATRIZ DE CALIFICACIÓN DE RIESGOS**

		Impacto		
		1	2	3
		Bajo	Medio	Alto
Probabilidad	Alto	3 Riesgo Moderado	6 Riesgo importante	9 Riesgo inaceptable
	Medio	2 Riesgo tolerable	4 Riesgo moderado	6 Riesgo importante
	Bajo	1 Riesgo aceptable	2 Riesgo tolerable	3 Riesgo moderado



A los ejes de probabilidad e impacto de la matriz se les ha asignado una escala. La definición de cada criterio se realiza a continuación:

#### Referente a la probabilidad:

- **Alto:** Es muy probable la materialización del riesgo o se presume que llegará a materializarse.
- **Medio:** Es probable la materialización del riesgo o se presume que posiblemente se podrá materializar.
- **Bajo:** Es poco probable la materialización del riesgo o se presume que no llegará a materializarse.

#### Referente al Impacto:

- **Alto:** Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.
- **Medio:** Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.
- **Bajo:** Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

#### Determinación de la escala para determinar el nivel del riesgo

La Matriz de Calificación de Riesgos, bajo el enfoque de probabilidad e impacto, permite establecer una métrica que se evidencia en una escala. La escala se obtiene con el cruce de los ejes de Probabilidad e Impacto y se clasifican de la siguiente manera:

- **Riesgo inaceptable:** Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Dirección.
- **Riesgo importante:** Se requiere atención de la Alta Dirección. Planes de tratamiento requeridos, implementados y reportados a los jefes de oficinas, unidades, entre otros.
- **Riesgo moderado:** Debe ser administrado con procedimientos normales de control. Su seguimiento se debe dar cada cuatro (04) meses.
- **Riesgo tolerable:** Menores efectos que pueden ser fácilmente remediados. Se administra con procedimientos rutinarios. Su seguimiento se debe dar cada seis (06) meses.
- **Riesgo aceptable:** Riesgo insignificante. No se requiere ninguna acción.

#### 7.4 Diseño del control

En esta etapa, se analizan los controles internos implementados, cuyo objeto es atenuar el impacto que tendría el riesgo en caso se materialice, tomando en consideración las características para su diseño.

Los controles, según el tipo pueden ser:

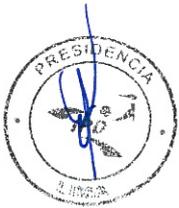
- **Controles preventivos:** Actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa. Sirven para frenar ciertas transacciones antes de su ejecución (Ejemplos: Revisión de firmas y saldo antes de efectuar el pago).
- **Controles detectivos:** Sirven para supervisar la ejecución del proceso. Ofrecen la segunda barrera de seguridad frente a los riesgos, pudiendo informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema,

monitorear, o alertar a los servidores. Se diseñan para alertar sobre la presencia de los riesgos, permitiendo tomar acciones inmediatas. (Ejemplos: Sistema de alarma, doble verificación de cálculos).

- Controles correctivos: Identifica desviaciones cuando el riesgo se ha materializado. Permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles actúan cuando ya se han presentado hechos que implican pérdidas para el IPD. (Ejemplos: Planes de contingencia, seguros).

Los controles, según su ejecución pueden ser:

- Manual: Actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa. Sirven para frenar ciertas transacciones antes de su ejecución (Ejemplos: Revisión de firmas y saldo antes de efectuar el pago).
- Automatizada: Son aplicados a través de sistemas de información automatizados. Aseguran la correcta captación de la información y procedimientos de autorización y aprobación por parte de los responsables.
- Combinada: Su aplicación es parcialmente automatizada y combina acciones de control manuales. (Ejemplo: Verificaciones de documentos, autorizaciones, registro de datos en aplicativos).



Los controles, según su documentación pueden ser:

- Documentado: Los controles están apoyados en documentos normativos actualizados (Manual de Organización y Funciones, manuales de procedimientos, circulares, directivas, entre otros).
- Desactualizada: Se cuenta con documentos normativos de respaldo a la aplicación de los controles, pero éstos son parciales y no detalla en forma clara y precisa el procedimiento de control y como se vienen ejecutando los mismos.
- Sin documentar: Los controles se realizan en base a la experiencia y al criterio del funcionario y no cuentan con documentación que lo sustente.



Los controles, según su periodicidad pueden ser:

- Continuos: Se aplica en forma constante cada vez que se ejecuta la transacción, operación o actividad; se debe considerar además si es adecuado o no que el control sea continuo.
- Periódicos: Pueden ser anuales, semestrales, mensuales, quincenales, semanales o diarios, dependiendo de la ejecución de las operaciones, transacciones o actividades: se debe considerar además si es adecuado o no que el control sea periódico-
- Esporádico: Se aplican en forma ocasional, de acuerdo al criterio del trabajador encargado.



Los controles, según su responsabilidad pueden ser:

- Asignada y formalizada: La responsabilidad del funcionario o servidor que ejecuta el control se encuentra definida y se sustenta en documentos normativos.
- Asignada no formalizada: Se ha definido el responsable de la ejecución del control, pero no cuenta con documento normativo que lo respalde.
- No asignada: No se ha definido el responsable de la ejecución del control, pudiendo ejecutarlo diversos funcionarios o servidores.

#### 7.5 Respuesta o tratamiento

La respuesta a los riesgos identificados involucra la definición de las posibles respuestas a implementarse. Estas consideran las siguientes estrategias:

- a) **Evitar**: La acción es tomada para evitar afrontar los riesgos, inclusive evitando realizar las actividades que pueden provocarlos.
- b) **Mitigar**: Implica llevar a cabo acciones para reducir la probabilidad o impacto del riesgo o ambos conceptos a la vez.
- c) **Transferir**: La probabilidad o impacto del riesgo se reducen compartiendo una parte del riesgo. Las técnicas más comunes incluyen la contratación de seguros, operaciones de cobertura o tercerización de una actividad.
- d) **Aceptar**: No se emprende ninguna acción que afecte a la probabilidad o el impacto del riesgo.

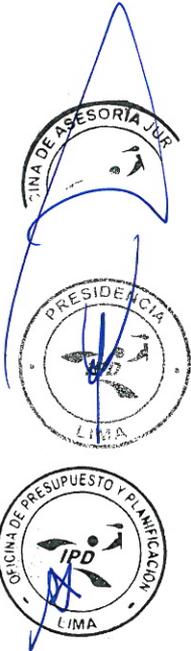
La respuesta a seguir busca llevar el riesgo a los niveles aceptados por el IPD. La elección de la estrategia debe ser sustentada y validada por el funcionario a cargo del objetivo institucional o proceso, considerando los siguientes criterios:

- a) **Evaluación del efecto sobre la probabilidad y el impacto del riesgo**: Al analizar las respuestas se puede tener en cuenta los eventos y tendencias pasadas y los posibles escenarios futuros.
- b) **Evaluación costo beneficio**: En algunos casos es difícil cuantificar los costos y beneficios de la respuesta al riesgo, debiendo emplearse métodos de mayor subjetividad, como el análisis de escenarios, la evaluación y ponderación de ventajas y desventajas, entre otras.

#### Priorización

El Comité de Riesgos del IPD, considerando la información remitida por los órganos y unidades orgánicas, dará su aprobación a la priorización de los riesgos identificados, a fin de ser incluido en el Plan de Gestión de Riesgos de la Entidad.

Luego de implementado el Plan de Acción, periódicamente el Comité de Riesgos deberá informar al Comité de Control Interno el resultado de reevaluar si el nivel de riesgo a sufrido alguna variación, debido a cambios en el contexto en el que se desarrollan las actividades del proceso/subproceso, a fin de adoptar las medidas necesarias con el objeto de mantener un nivel adecuado.



## 7.6 Información y comunicación

La información pertinente se identifica, capta y comunica en forma oportuna, en un marco de tiempo que permite a los funcionarios y servidores llevar a cabo sus responsabilidades.

La información que deberá remitir el Comité de Riesgos del IPD, a la Alta Dirección y al Comité de Control Interno es la siguiente:

- Informe semestral del Plan de Gestión de Riesgos, en la primera sesión del Comité de Control Interno del mes siguiente a la fecha de corte.
- Informes solicitados por la Alta Dirección.
- Informes de riesgos de nuevos servicios, productos o cambios importantes y significativos para el cumplimiento de los objetivos del IPD.

La información que deberán remitir los órganos y unidades orgánicas del IPD es la siguiente:

- Informe trimestral de los riesgos del área, hasta el quince (15) del mes siguiente a la fecha de corte.
- Informes de riesgos de nuevos servicios, productos o cambios importantes y significativos para el cumplimiento de los objetivos del IPD.
- Información contenida en el Plan de Gestión de Riesgos del IPD.



## 7.7 Monitoreo

Es el proceso que consiste en la evaluación del adecuado funcionamiento de la gestión de riesgos y la implementación de las acciones que se requieran.

El monitoreo incluye evaluaciones internas a cargo de los servidores y funcionarios del IPD involucrados y externas a cargo de la Contraloría General de la República y otros.



## 7.8 Tolerancia al riesgo

El IPD, a través de la Alta Dirección, establece los niveles de tolerancia a los riesgos identificados y contenidos en el Plan de Gestión de Riesgos Institucional, así como los parámetros que todos los órganos y unidades orgánicas deben tomar en cuenta para el desarrollo de sus actividades dentro de su marco de toma de decisiones, ya sean administrativas, tecnológicas, de seguridad de control u otras.



Los niveles cambiarán en función a los cambios que se den en el contexto externo e interno que afecte al IPD, razón por la cual deberán ser revisados periódicamente a fin de validar su vigencia. Estos niveles se constituyen en elementos que impulsan la adecuada gestión del IPD en la consecución de sus objetivos estratégicos.

## 7.9 Sistema de gestión de la seguridad de la información

Como parte de una adecuada gestión del riesgo, el IPD implementa un sistema de gestión de seguridad de la información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de la información.

Al ser parte de la gestión de riesgo, la gestión de la seguridad de la información, a través de las evaluaciones periódicas y actualizaciones del inventario de activos críticos, dotará de



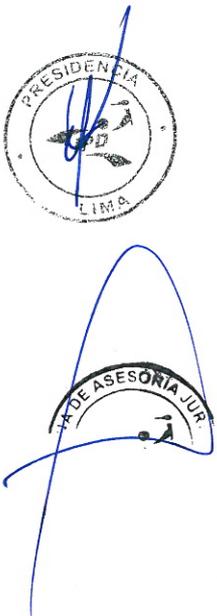
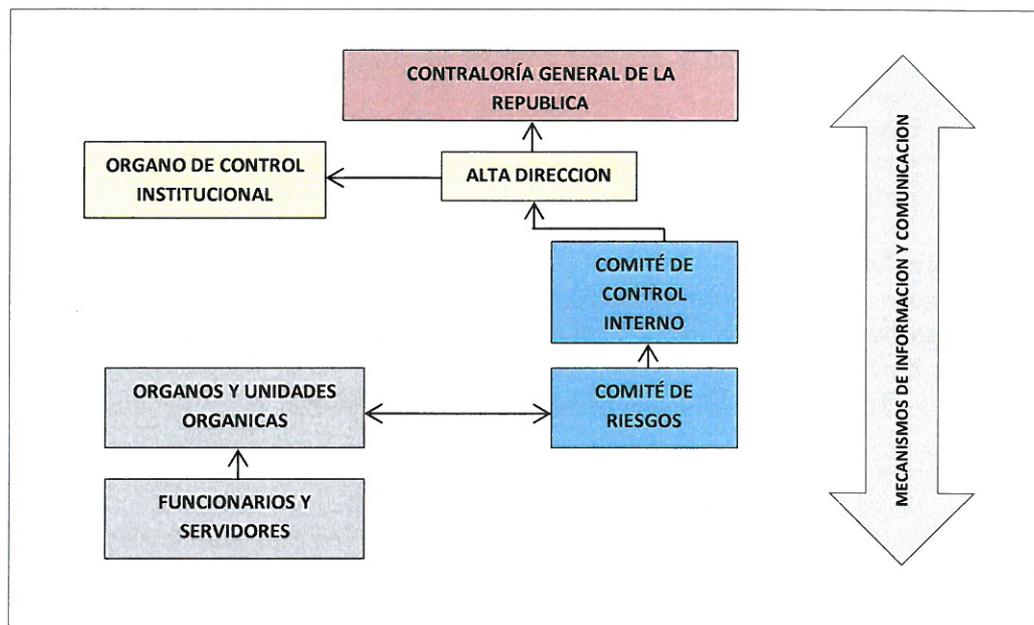
información adicional para la gestión de riesgos, la misma que deberá tener un tratamiento con los riesgos ya identificados.

### 7.10 Capacitación para la gestión de riesgos

Con el fin de fomentar la cultura de gestión de riesgos, difundir la política y normas e impulsar la aplicación de la metodología establecida por el IPD, la Oficina General de Administración, a través de la Unidad de Personal, deberá implementar un programa de capacitación en riesgos, que deberá formar parte del Plan de Desarrollo de las Personas del IPD.

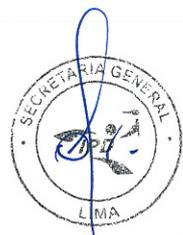
### 7.11 Responsabilidades

El desarrollo de las actividades vinculadas a la gestión del riesgo, involucra la participación de la Alta Dirección, el Comité de Control Interno, el Comité de Riesgos y los órganos y unidades orgánicas del IPD. En tal sentido, la estructura organizacional relacionada a la gestión de riesgos es la siguiente:



#### a) **Alta Dirección:**

- Aprobar las políticas, lineamientos, manuales, metodologías, directivas y demás instrumentos de gestión de riesgos.
- Asignar los recursos necesarios para la adecuada gestión de riesgos, a fin de contar con la infraestructura, metodología y estructura organizacional aprobados.
- Aprobar el nivel de tolerancia y grado de exposición al riesgo que el IPD está dispuesto a asumir en el desarrollo de su misión.
- Establecer incentivos que fomenten la adecuada gestión de riesgos.
- Conocer los principales riesgos afrontados por la Entidad, estableciendo adecuados niveles de tolerancia a los mismos.
- Obtener un aseguramiento razonable que el IPD cuenta con una efectiva gestión de riesgos y que los principales riesgos identificados se encuentren bajo control dentro de los límites que se han establecido.



**b) Comité de Control Interno:**

- Revisar y proponer la aprobación de las políticas, lineamientos, manuales, metodologías, directivas y demás instrumentos de gestión de riesgos, así como las modificaciones que se realicen a los mismos.
- Evaluar y proponer el nivel de tolerancia y grado de exposición al riesgo que el IPD está dispuesto a asumir en el desarrollo de su misión.
- Decidir las acciones necesarias para la implementación de las acciones de corrección requeridas, en caso existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.
- Aprobar la toma de exposiciones al riesgo que involucren variaciones significativas en el perfil de riesgo del IPD.
- Realizar el seguimiento del cumplimiento de la Política de Administración de Riesgos.
- Proponer mejoras en la Gestión de Riesgos.

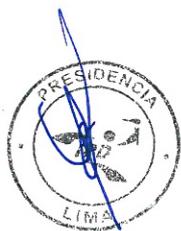
**c) Comité de Riesgos:**

- Promover y facilitar la asistencia a los órganos y unidades orgánicas del IPD para la aplicación de la metodología de gestión del riesgo.
- Evaluar el riesgo a nivel de la Entidad y proponer acciones para el tratamiento de los eventos de riesgo a los que está expuesto el IPD de acuerdo a la metodología establecida.
- Proponer mejoras en la gestión de riesgos.
- Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo.

**d) Directores y Jefes:**

Tienen la responsabilidad de gestionar los riesgos de su competencia, a través de la identificación, tratamiento y control de los mismos, relacionados al logro de los objetivos de las dependencias a su cargo, dentro de las políticas de riesgo, límites, metodología y procedimientos establecidos. En tal sentido, les compete:

- Participar en la gestión de riesgos, lo que implica verificar y asegurar el cumplimiento de las funciones y responsabilidades establecidas.
- Autorizar, monitorear y disponer las acciones necesarias para la ejecución de planes de acción de los riesgos críticos identificados en los procesos a su cargo.
- Consolidar y validar la información a ser remitida para el llenado del Plan de Gestión de Riesgos.
- Presentar periódicamente al Comité de Control Interno, el estado de situación de la gestión de riesgos de su dependencia y de ser el caso, comunicar las causas o factores limitantes en la mitigación de sus riesgos críticos.
- Disponer la ejecución de acciones a efectos de asegurar que el personal a su cargo reciba la capacitación vinculada a la gestión de riesgos.
- Validación y aceptación de las pérdidas por eventos de riesgo reportadas por las dependencias a su cargo.
- Aprobación del reporte de evento de interrupción respecto a los productos y servicios que lidera.
- Aprobación de las estrategias del plan de continuidad operativa, así como los tiempos máximos de recuperación por cada producto o servicio que lidera.
- Velar por el cumplimiento de las políticas de seguridad de la información, identificación y reporte de incidentes y eventos de seguridad de la información, manteniendo actualizado el inventario de activos y clasificación de la información.



**8. DISPOSICION COMPLEMENTARIA**

La Oficina de Presupuesto y Planificación, a través de la Unidad de Organización y Métodos, será la encargada de absolver cualquier duda o consulta que surja respecto a la aplicación del presente instrumento.

