POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

INDERBU

INSTITUTO DE LA JUVENTUD, EL DEPORTE Y LA RECREACIÓN DE BUCARAMANGA

INDERBU
Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga

1. INTRODUCCIÓN

El presente documento establece la Política de Administración de Riesgos del Instituto de la Juventud el Deporte y Recreación de Bucaramanga-Inderbu. Así como, los lineamientos para la identificación, y valoración de los riesgos que puedan afectar el cumplimiento de la misión, de los objetivos estratégicos, la gestión de los procesos y la satisfacción de los grupos de interés, de acuerdo con las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de la línea estratégica y líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI – Dimensión 7 Control Interno y la Guía para la administración del riesgo expedida por el Departamento Administrativo de la Función Pública.

DECLARACIÓN POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS DEL INDERBU

La Alta Dirección del Inderbu y el equipo humano de la entidad está comprometido para llevar a cabo una gestión integral de riesgos que facilite el cumplimiento de la misión, los objetivos estratégicos, objetivos de los procesos y la satisfacción de los grupos de interés, llevando a cabo la identificación de riesgos de gestión por proceso, los riesgos de seguridad digital, su análisis, valoración y formulación de los planes de tratamiento de riesgos o acciones para prevenir su ocurrencia o mitigar el impacto.

Las políticas de manejo de riesgo aplican a todos los procesos del Inderbu y establecen las opciones para el tratamiento de los riesgos. Los riesgos de corrupción son inaceptables y en consecuencia no se pueden asumir. El tratamiento general para los riesgos corresponde a la implementación de acciones que conlleven a reducir, evitar, compartir, aceptar o transferir y serán individuales para cada uno de los riesgos identificados. Las acciones o controles se formularán considerando su viabilidad técnica, económica y legal.

2. OBJETIVO GENERAL

Establecer los lineamientos para la administración de los riesgos de gestión y seguridad digital asociados a la gestión institucional.

2.1. OBJETIVOS ESPECÍFICOS

- Comunicar a todos los niveles del instituto los lineamientos para la administración del riesgo, para promover su aplicación.

- Fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución.

- Asignar responsabilidades frente a la administración del riesgo.

3. ALCANCE

La Política para la Administración de Riesgos es aplicable a todos los procesos del Sistema de Gestión del Instituto, así como a todas las dependencias y niveles.

Los riesgos de Gestión por proceso, se establecerán de acuerdo con los lineamientos que emita el Departamento Administrativo de la Función Pública – DAFP, a través de la guía de riesgos.

Los riesgos del Sistema de Seguridad y Salud en el Trabajo, Seguridad digital y los riesgos del Sistema de Gestión Ambiental, se establecerán de acuerdo con la normatividad aplicable en cada caso.

4. TÉRMINOS Y DEFINICIONES

A continuación, se relacionan algunos de los conceptos, necesarios para la comprensión de la metodología señalados por el Instituto de la Juventud el Deporte y la Recreación de Bucaramanga -Inderbu.

Activo de Información: Un activo es cualquier elemento que tenga valor para la entidad, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO- que utiliza la entidad para su funcionamiento.

Administración de Riesgos: Es el proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. Incluye el conjunto de elementos de control y sus interrelaciones, para que la UPME maneje los eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La Administración del riesgo contribuye a generar la cultura de autocontrol y autoevaluación al interior de la Unidad.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Contexto Interno: Es el entorno interno en el cual la organización busca definir y lograr sus objetivos.

Contexto Externo. Es el entorno externo en el cual la organización busca definir y lograr sus objetivos.

Control: Medida que permite reducir o mitigar un riesgo. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DAFP: Departamento Administrativo de la Función Pública.

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Presencia o cambio de un conjunto particular de circunstancias.

Gestión del Riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Son las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Nivel o Zona del Riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan para el Tratamiento o Gestión del Riesgo: Conjunto de acciones preventivas que se encuentran dentro del marco de referencia para gestionar los riesgos, en esta se definen componentes como los responsables, los recursos y los métodos que se van a utilizar para mitigar, eliminar o asumir los riesgos.

Política de Operación: Aquella directriz general que reconoce el marco legal que rige y aplica al Inderbu y la cual es desarrollada a través de la definición de los procesos, los procedimientos y las guías internas, que involucran las líneas de acción, los objetivos, actividades, tareas y controles que permiten el logro del objeto misional de la entidad y el cumplimiento de las responsabilidades con el estado.

Política de administración del riesgo: Declaración de la entidad e intenciones generales de la organización con respecto a la gestión del Riesgo.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.

Riesgo Aceptable: Riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legales.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgos 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 comunidad.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia en acciones de la dirección para modificar su probabilidad e impacto.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgos Operativos: Comprende riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgo Residual: Riesgo remanente después del tratamiento del riesgo. Es el riesgo que permanece después de que la dirección haya realizado sus acciones para reducir el impacto y la probabilidad de un acontecimiento adverso, incluyendo las actividades de control en respuesta a un riesgo.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

La administración del riesgo depende de la participación de la Alta dirección, servidores públicos y contratistas; por esto se deben identificar las responsabilidades de acuerdo con las líneas de defensa que se presentan a continuación:

- **Oficial de Seguridad**

El Oficial de Seguridad de la Información es el responsable de planificar, desarrollar, controlar, gestionar y/o coordinar las estrategias de seguridad de la información, con el fin de mantener la confidencialidad, integridad y disponibilidad; y de promover el diseño, establecimiento, implementación, operación, revisión, mantenimiento y mejora continua de la gestión en seguridad de la información.

- **Especialista de Seguridad Informática**

El especialista de Seguridad Informática es responsable de gestión y administración de la infraestructura de seguridad informática, gestionar la remediación de vulnerabilidades técnicas y monitorear los eventos de seguridad de la plataforma tecnológica, así como coordinar las acciones de respuesta y recuperación al incidente se seguridad de la información.

- **Coordinador de Protección de Datos**

El Coordinador de Protección de Datos es responsable de velar por la implementación efectiva de las políticas y procedimientos del programa de protección de datos personales para dar cumplimiento a las normas sobre protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro del INDERBU.

ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación, valoración y definición de controles para el tratamiento y seguimiento.

NIVELES DE ACEPTACIÓN AL RIESGO

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización. Los riesgos de gestión inherentes, ubicados en la zona de riesgos “baja” pueden ser aceptados y por lo tanto no es necesario establecer controles. Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes y realizar su seguimiento.

El mapa de calor de riesgos permite visualizar los riesgos de gestión en las zonas de riesgos definidas (Baja, Moderada, Alta, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a buscar o retener (apetito del riesgo) en función del impacto de estos en la Unidad. Los riesgos que se encuentren en zona baja se aceptan y se continúa el monitoreo.

El mapa de calor de riesgos permite visualizar los riesgos de seguridad digital en las zonas de riesgos definidas (Bajo, Moderado, Alto, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención; estableciendo un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociado a los activos de información sin importar el nivel de criticidad que tienen para la entidad. Los riesgos de seguridad digital que se encuentren en las zonas Bajo y Moderado se aceptan y se continúa el monitoreo.

Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento. Los riesgos que se encuentran en las zonas más altas son los que se priorizan orientando los esfuerzos y acciones para mejorar su administración de riesgos.

NIVELES PARA CALIFICAR EL IMPACTO.

Las tablas de calificación del impacto definidas para los Riesgos de Gestión en Seguridad Digital se definen así:

Tabla. Valoración de la Frecuencia del Riesgo

IMPACTO		
No.	**Rango**	**Formula**
3	Severo	Supera o incumple el rango permitido por los requisitos establecidos (Normatividad Legal – Acuerdos – Disposiciones establecidas por la entidad o partes interesadas)
2	Moderado	Se encuentra dentro de los rangos o 13arámetros establecidos (Normatividad Legal – Acuerdos – Disposiciones establecidas por la entidad o partes interesadas)
1	Leve	Supera las expectativas de los rangos o 13arámetros establecidos (Normatividad Legal – Acuerdos – Disposiciones establecidas por la entidad)

Tabla. Valoración del Impacto del Riesgo.

ALCANCE		
No.	**Rango**	**Formula**

3	Global	Eventos que Superan los límites del área donde se ejecutan las actividades propias de la entidad
2	Local	Eventos que están dentro de los límites donde se ejecutan las actividades propias de la entidad
1	Puntual	Eventos que suceden puntualmente y que se pueden tratar dentro de los límites donde se ejecutan las actividades propias de la entidad

Tabla. Valoración del Alcance del Riesgo.

<table>
<tr><td colspan="4">FRECUENCIA</td><td rowspan="2">240 días hábiles</td></tr>
<tr><td colspan="3">No.</td><td>Rango</td><td>Formula</td></tr>
<tr><td colspan="3">3</td><td>Alta</td><td>Entre > 0,5</td><td rowspan="4"># de Veces que ocurre la actividad/# días hábiles trabajados al año</td></tr>
<tr><td colspan="3">2</td><td>Media</td><td>Entre <= 0,5 y >0,2</td></tr>
<tr><td colspan="3" rowspan="2">ZONA DEL RIESGO
<table><tr><th>No.</th><th>Rango</th><th>Descripción</th><th>Rango</th></tr><tr><td>> = 2,5</td><td>ALTO</td><td>La zona de riesgo supera los límites establecidos en cuanto a impacto y alcance afectando las actividades que realiza la entidad para lo cual se deben implementar o establecer controles adicionales</td><td>ALTO</td></tr></table></td><td>Bajo</td><td>Entre <=0,2</td></tr>
</table>

> 2,0 a < 2,5	**MEDIO**	La zona de riesgo se encuentra en los limites permisibles en cuanto a impacto y alcance, para lo cual se debe evitar que el riesgo se materialice implementando los controles adecuados	**MEDIO**
< = 2,0	**BAJO**	La zona de riesgo se encuentra dentro de los rangos establecidos por la entidad en cuanto alcance e impacto permitiendo asumir el control del riesgo.	**BAJO**

1

Criterios zona de Riesgo

Criterios de valoración del control

Criterios valoración del riesgo

VALORACION DEL RIESGO			
No.	**Rango**	**Descripción**	**Rango**
> = 6	**INACEPTABLE**	El control con el que actualmente se cuenta para la mitigación del riesgo no asegura que la materialización del mismo no se presente, por lo cual la entidad debe adelantar las acciones inmediatas con el fin de asegurar la efectividad del control (establecer el control, reevaluarlo, establecer unos nuevos, entre otros).	**INACEPTABLE**
>3 y <6	**MODERADO**	El Control existente debe evaluarse mediante auditorias o seguimiento permanente con el fin de garantizar el resultado satisfactorio del proceso mediante la mitigación del riesgo.	**MODERADO**
<=3	**ACEPTABLE**	Ya la entidad evaluó el control y se está asegurando el resultado del proceso, el riesgo no se ha materializado y mediante la aplicación de estos controles se puede asegurar que el riesgo es aceptable y se controlara a través de seguimiento de auditorías de gestión y externas por parte de los entes de control.	**ACEPTABLE**

VALORACION DEL CONTROL			
No.	**Rango**	**Criterio**	**Rango**
3	**INEFECTIVO**	El control no existe, o existe pero no se aplica, o existe y se aplica pero el mismo no es efectivo.	**INEFECTIVO**
2	**EN PRUEBA**	El Control existe y está en implementación, pero aún no se evidencia su efectividad.	**EN PRUEBA**
1	**EFECTIVO**	El control existe y se aplica de manera efectiva, asegurando la no materialización del riesgo	**EFECTIVO**

TRATAMIENTO DE RIESGOS

Es la respuesta que define la primera línea de defensa de la Entidad para mitigar los riesgos. Las opciones del tratamiento del riesgo incluyen aceptar, reducir, evitar o compartir los riesgos según se describe a continuación:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos. Por lo general conlleva a la implementación de controles.

Evitar el Riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Transferir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o
compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

10. PERIODICIDAD PARA EL SEGUIMIENTO DE ACUERDO CON EL NIVEL DE RIESGO RESIDUAL

10.1 Riesgos de Gestión y Corrupción

● Se realizarán actividades de seguimiento cuatrimestral por parte de los responsables de proceso para determinar la efectividad de los controles asociados a los riesgos y sobre las acciones de tratamiento sobre el riesgo residual. El grupo integrado de trabajo de Planeación brindará el apoyo requerido en su rol de segunda línea de defensa.

● El reporte del seguimiento se realizará de acuerdo con los lineamientos que defina el grupo integrado de trabajo de Planeación.

● Los responsables de proceso deben informar al grupo integrado de trabajo Planeación, cuando ocurran cambios del entorno o del proceso que puedan generar ajustes en cualquiera de las etapas de la administración del riesgo.

● El grupo integrado de trabajo de Planeación, consolida la gestión del riesgo e informa a la alta dirección sobre su estado.

● La Asesora de Control Interno realiza la evaluación independiente de la administración del riesgo - mapas de riesgos de corrupción de manera cuatrimestralmente de acuerdo con los términos legales y a los riesgos de gestión de acuerdo con las auditorías que adelante.

● Los mapas de riesgo se deben establecer o actualizar para cada vigencia, teniendo en cuenta que cada vigencia puede tener contextos diferentes. Igualmente, se podrán actualizar riesgos específicos en caso de requerirse por solicitud de los responsables de procesos o por temas que así lo ameriten.

10.2. Riesgos de Seguridad Digital

● El reporte del seguimiento se realizará de acuerdo con los lineamientos que defina el Jefe de Seguridad de la información.
● Los responsables de proceso deben informar al Jefe de Seguridad de la información, cuando ocurran cambios del entorno o del proceso que puedan generar ajustes en cualquiera de las etapas de la administración del riesgo.

● La Asesora de Control Interno realiza la evaluación independiente de la administración del riesgo - mapas de riesgos de seguridad digital de acuerdo con los términos legales en las auditorías que adelante.

2. CONTROL DE CAMBIOS.

VERSIÓN	DESCRIPCIÓN Y/O MODIFICACIONES	FECHA
01	Creación del documento	**11/12/2023**

CONTROL DE DOCUMENTOS			
ELABORÓ: Nombre: Mónica Rocío Niño Entralgo Cargo: CPS Sistemas	**REVISÓ:** Nombre: Tatiana Palencia Cáceres Cargo: Subdirectora Administrativa y Financiera	**APROBÓ:** Nombre: Comité Institucional de Gestión y Desempeño	**FECHA DE APROBACIÓN:** **11/12/2023**