TABLA DE CONTENIDO

1. OBJETIVO

Establecer los lineamientos institucionales para desarrollar una administración estructurada, sistemática, oportuna y efectiva de los riesgos de gestión, corrupción y seguridad digital que afectan el logro del objetivo misional del Ministerio del Deporte, orientado a "formular, adoptar, dirigir, coordinar, inspeccionar, vigilar, controlar y ejecutar la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física para promover el bienestar, la calidad de vida, así como contribuir a la salud pública, a la educación, a la cultura, a la cohesión e integración social, a la conciencia nacional y a las relaciones internacionales, a través de la participación de los actores públicos y privados" definido en la Ley 1967 de 2019; con el propósito de guiar a los procesos de la Entidad en la identificación, valoración, definición de acciones de tratamiento y seguimiento a sus riesgos, para gestionarlos al nivel aceptable definido por la entidad.

Para lo anterior, la administración de riesgos del Ministerio del Deporte se realizará bajo los principios de:

- Generar valor en la gestión de los procesos de la Entidad
- Aportar a la toma de decisiones basada en la información disponible relacionada con la gestión de riesgos
- Desarrollar una administración sistemática, estructurada, oportuna y efectiva
- Trasparente e inclusiva para todos los responsables en la gestión de riesgos
- Ser dinámica, reiterativa y sensible a los cambios en el contexto
- Mejora continua del Ministerio del Deporte.

2. ALCANCE

El presente documento define los lineamientos para la administración de riesgos de gestión, corrupción y seguridad digital del Ministerio del Deporte, los cuales se extienden y son aplicables para la gestión y el control de riesgos asociados a los procesos en materia del Deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física.

3. GLOSARIO Y CONSIDERACIONES BÁSICAS

3.1. Glosario

- **Aceptación del Riesgo:**
  Decisión frente al tratamiento de un riesgo, en la cual no se adoptan acciones de control que afecten la probabilidad o impacto de riesgo. Para los riesgos de corrupción no habrá ningún tipo de aceptación.

- **Activo:**
  En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Actividades de Control:**
  Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

- **Amenazas:**
  Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Apetito al riesgo:**
  Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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

- **Compartir el Riesgo:**
  Decisión frente al tratamiento de un riesgo de gestión, corrupción o seguridad digital que es muy difícil de reducir a un nivel aceptable, en la cual se comparte la gestión del mismo con otra parte interesada, para que sea gestionado con mayor eficacia. Cabe resaltar que los riesgos se comparten, pero no se transfiere la responsabilidad sobre estos.

- **Confidencialidad:**
  Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **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 Estratégico:**
  Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones del entorno de la entidad, tanto de carácter social, económico, cultural, de orden público, político, legal, tecnológicos entre otros.

- **Control:**
  Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Disponibilidad:**
  Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Enlace:**
  Persona asignada por cada líder de proceso, responsable de desplegar los lineamientos definidos en la presente política, para la implementación de la metodología de la administración del riesgo en los respectivos procesos.

- **Evitar el Riesgo:**
  Decisión frente al tratamiento de un riesgo, de abandonar las actividades que dan lugar al riesgo considerado extremo para la Entidad.

- **Gestión del Riesgo:**
  Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Impacto:**
  Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:**
  Propiedad de exactitud y completitud.

- **Líneas de Defensa:**
  Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

- **Mapa de Riesgos:**
  Documento con la información resultante de la gestión del riesgo.

- **Probabilidad:**
  Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

- **Reducir el Riesgo:**
  Decisión frente al tratamiento de un riesgo, en la cual se adoptan medidas para reducir la probabilidad y/o impacto del riesgo y conlleva a la implementación de controles.

- **Riesgo:**
  Evento probable que puede afectar el desarrollo normal de las funciones de la Entidad y el logro de sus objetivos.

- **Riesgo de Gestión:**
  Evento probable que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo de Corrupción:**
  Evento probable en el cual, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **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.

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

- **Riesgo Residual:**
  Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **Tolerancia al Riesgo:**
  Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- **Vulnerabilidad:**
  Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

3.2. Consideraciones Básicas

El Ministerio del Deporte, en el marco de la política de administración del riesgo, parte de la alineación al Plan Nacional de Desarrollo vigente, con los objetivos estratégicos de la Entidad y a su vez con los objetivos de los procesos establecidos en el Sistema Integrado de Gestión Institucional; base sobre la cual se implementarán las acciones tendientes a mitigar los riesgos identificados a niveles aceptables; lo anterior, bajo los parámetros del Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno - MECI y la Guía de Administración del Riesgo vigente.

En la presente política de administración del riesgo, se propende por la articulación de los riesgos de gestión, corrupción y de seguridad digital que se pueden llegar a presentar en la Entidad, para lo cual serán debidamente identificados y registrados en el formato de mapa de riesgos, establecido para tal fin.

El Ministerio, para administrar adecuadamente sus riesgos establece las acciones para aceptarlos, reducirlos, evitarlos o compartirlos; asimismo, en caso de materialización de algún riesgo, se definen y ejecutan los respectivos planes de tratamiento que permitan mitigar el impacto sobre los objetivos de la Entidad.

4. NIVELES DE ACEPTACIÓN DEL RIESGO

De acuerdo con lo establecido por la Alta Dirección a través del Comité Institucional de Coordinación de Control Interno, el Ministerio del Deporte contará con los siguientes niveles de aceptación, de acuerdo con la zona en la cual se ubiquen los riesgos; la cual estará determinada por la probabilidad de ocurrencia del riesgo y el impacto que generaría sobre los objetivos estratégicos:

Tabla No. 1. Niveles de Aceptación del Riesgo en el Ministerio del Deporte.

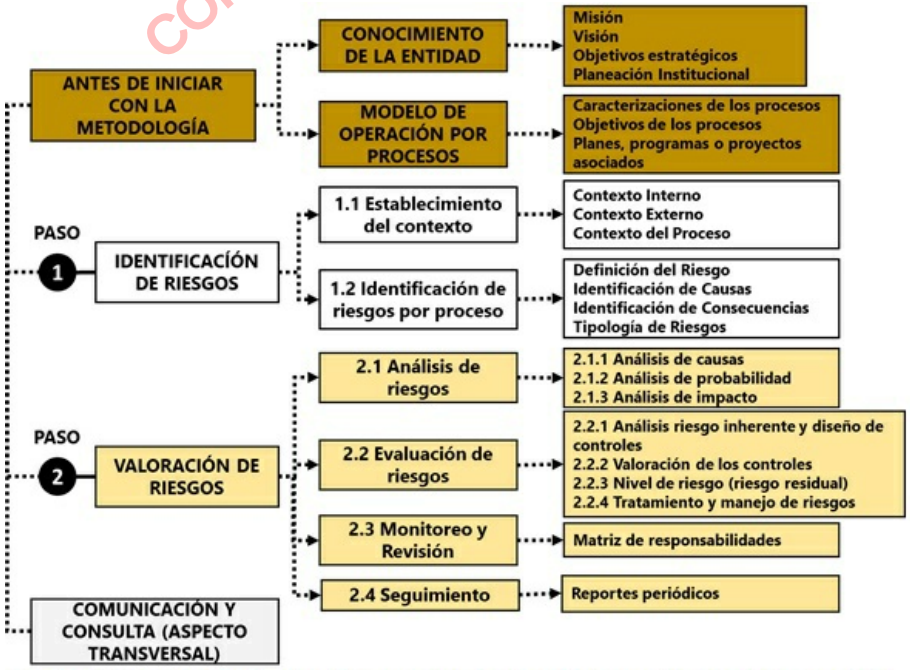
Clasificación del Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión Riesgos de Seguridad Digital	Baja	Considerando que son riesgos que presentan una probabilidad reducida de presentarse en la gestión de los procesos, y que de llegarse a materializar no afectaría significativamente el cumplimiento de la estrategia de la Entidad; **el Ministerio del Deporte determina aceptar** los riesgos que se ubiquen en zona baja, no obstante, estos serán controlados a través de la definición de puntos de control en el desarrollo de las actividades propias relacionadas de cada proceso.
Riesgos de Gestión Riesgos de Seguridad Digital	Moderada Alta Extrema	Los riesgos ubicados en las zonas moderada, alta y extrema representan mayores niveles de probabilidad e impacto que podrían incidir directamente sobre los objetivos estratégicos de la Entidad, de tal manera **el Ministerio del Deporte no tendrá ningún nivel de aceptación** sobre los riesgos ubicados en dichas zonas, por tal razón la Entidad establecerá actividades de control de carácter preventivo y/o detectivo que permitan reducir, compartir o evitar el riesgo; estas actividades serán administradas mediante los mapas de riesgos y serán monitoreadas constantemente por parte de los líderes de proceso, generando reportes cuatrimestrales de su monitoreo; a su vez la Oficina Asesora de Planeación desarrollará monitoreo y evaluación de los controles y la gestión del riesgo. Asimismo, la Oficina de Control Interno proporcionará un aseguramiento objetivo sobre la efectividad de las actividades de la administración del riesgo.
Riesgos de Corrupción	Moderada Alta Extrema	Considerando el impacto que generan los riesgos de corrupción, **el Ministerio del Deporte no tendrá aceptación de este tipo de riesgos**, por lo tanto, se establecerán los controles tendientes a prevenir, detectar y/o mitigar los impactos por su materialización; de igual manera, serán administrados por la Entidad a través del mapa de riesgos de corrupción establecido para tal fin. Para los riesgos de corrupción que se clasifiquen en zonas moderada, alta y extrema, se establecerán actividades de control que permitan reducir, compartir o evitar estos riesgos; y contarán con monitoreo constante por parte de los líderes de proceso, generando reportes cuatrimestrales de su monitoreo. La Oficina Asesora de Planeación realizará monitoreo a los riesgos de corrupción y asimismo la Oficina de Control Interno desarrollará el seguimiento cuatrimestral al mapa de riesgos de corrupción para verificar la efectividad de los controles.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

5. METODOLOGÍA DE ADMINISTRACIÓN DEL RIESGO

A partir de la presente política se establecen los lineamientos y directrices para la implementación de acciones para la administración de riesgos de gestión, corrupción y seguridad digital, enmarcadas en las etapas de identificación y valoración de riesgos. Para lo anterior, la Entidad adopta como referente la metodología definida en la guía vigente para la administración del riesgo y el diseño de controles en entidades públicas, establecida por la Función Pública , descrita en la siguiente imagen:

Imagen No. 1. Metodología Administración del Riesgo.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

Antes de Iniciar con la Metodología

Para dar inicio a la implementación de la metodología para la administración del riesgo en el Ministerio del Deporte, se requiere que los líderes de proceso y sus equipos de trabajo cuenten con un conocimiento general de la Entidad, es decir, deben entender el funcionamiento de la misma y su entorno; para lo anterior, un marco de referencia será la Ley 1967 de 2019 “Por la cual se

transforma el Departamento Administrativo del Deporte, La Recreación, la Actividad Física y el Aprovechamiento del Tiempo Libre (Coldeportes) en el Ministerio Del Deporte", en la que se define la misión o razón de ser de la Entidad y su estructura.

Asimismo, se debe considerar la visión en la cual se define la proyección a largo plazo de la Entidad y los objetivos estratégicos definidos para el cumplimiento de la misión, información que se encuentran en la plataforma estratégica del Ministerio del Deporte; por último, la planeación institucional, que corresponde a las estrategias definidas por la Entidad en el marco del Plan Nacional de Desarrollo.

Por otra parte, se debe considerar el modelo de operación por procesos vigente adoptado en el Ministerio del Deporte, el cual se puede consultar en la sección de Servicio al ciudadano – Transparencia y Acceso a la Información Pública – 3 Estructura Orgánica y de Talento Humano – Misión y Visión, de la página web de la Entidad; con el fin de tener el conocimiento detallado de la operación y las interrelaciones de los procesos orientados a satisfacer las necesidades de los grupos de valor de la Entidad.

Adicionalmente, para iniciar la implementación de la metodología, cada líder de proceso establecerá un enlace, preferiblemente un servidor público vinculado a la planta de la Entidad, quien será el encargado de ejercer las siguientes funciones:

- Interlocutor del proceso en todos los requerimientos relacionados con la administración del riesgo.

- Desplegar los lineamientos para la implementación de la metodología de administración del riesgo en el respectivo proceso.

- Asistir a las reuniones programadas por la Oficina Asesora de Planeación y /o demás áreas relacionadas con la administración del riesgo.

- Trasmitir a los colaboradores de las dependencias, las iniciativas y conocimientos adquiridos en las capacitaciones y/o reuniones realizadas.

5.1. Identificación de Riesgos

Previo a la identificación de riesgos, la Entidad a través de Oficina Asesora de Planeación como segunda línea de defensa, realizará el análisis de los objetivos estratégicos y de los procesos, con el fin de asegurar la alineación de los mismos con la misión y visión institucional.

La etapa de identificación se compone de dos aspectos: el establecimiento del contexto y como tal la identificación de riesgos propiamente dicha.

5. 1. 1. Establecimiento del Contexto

Es la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo; la definición del contexto se desarrolla tanto a nivel interno como externo de la Entidad, además del contexto en el cual opera el proceso y la identificación de los activos de seguridad digital; lo anterior, con base en la tabla No. 2.

Tabla No. 2. Factores para contexto externo, interno y de proceso.

Contexto	Factores
Externo	**Políticos**: cambios de gobierno, legislación, políticas públicas, regulación.
	Económicos y Financieros: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Sociales y Culturales: demografía, responsabilidad social, orden público.
	Tecnológicos: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Ambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Legales y Reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
Interno	**Financieros**: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	Personal: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	Estratégicos: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	Comunicación interna: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
	Cultura Organizacional: conjunto específico de normas, valores, tradiciones, conductas, creencias y experiencias que caracterizan al personal de la Entidad y se manifiestan en sus comportamientos.
Del Proceso	**Diseño del Proceso**: claridad en la descripción del alcance y objetivo del proceso.
	Interacciones con otros Procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la Entidad.
	Procedimientos Asociados: pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del Proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los Procesos: efectividad en los flujos de información determinados en la interacción de los procesos.
	Activos de Seguridad Digital del Proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 4.

- Contexto Interno: ambiente interno en el cual la organización busca alcanzar sus objetivos, son aspectos y características propias de la Entidad que inciden en su operación.

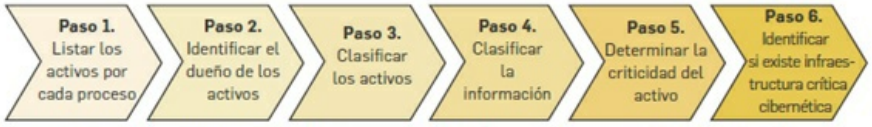
- Contexto Externo: es el ambiente externo en el cual la Entidad busca alcanzar sus objetivos, es decir, son factores que no están bajo el control de la Entidad y que inciden en su funcionamiento.

Para la definición del contexto externo e interno, se debe considerar la transición del Departamento Administrativo del Deporte, la Recreación, la Actividad Física y el Aprovechamiento del Tiempo libre – Coldeportes a Ministerio del Deporte, lo cual denota cambios para la Entidad y a su vez incide en la identificación de las causas de riesgos.

- Contexto del Proceso: son los factores propios de cada uno de los procesos, como su estructura, objetivo y alcance dentro de la Entidad, que denotan el ambiente en el cual el proceso busca alcanzar sus objetivos. Adicionalmente, se deben identificar los activos de información por proceso, como factor asociado al contexto del proceso.

La identificación de los activos de información, se realizará con el acompañamiento del GIT Tecnología de la Información y las Comunicaciones y se desarrollará atendiendo a los pasos descritos en la imagen No. 2, bajo los lineamientos establecidos para la gestión del riesgo de seguridad digital definido en la sección 4.1.6 del anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

Imagen No. 2. Pasos para la identificación de Activos de Información.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

Los activos de seguridad digital se plasmarán en el documento “Inventario de Activos de Seguridad Digital MINDEPORTE” que se encuentra en el servidor del GIT TIC’s; para seguir el adecuado proceso de identificación de los riesgos de la Entidad. Este documento se encuentra caracterizado de la siguiente manera:

• Identificación del proceso al cual se asocian los activos de seguridad digital

• Nombre del activo

• Descripción del activo de seguridad digital

• Dueño del activo (encargado de proteger el activo)

• Tipo de activo (activo de información, activo de software, activo físico, imagen y reputación, personas o servicios).

• Clasificación de la información (Uso Interno o público)

• Niveles de criticidad respecto a confidencialidad, integridad y disponibilidad de la información.

• Nivel de criticidad general del activo

Cada uno de los procesos deberá efectuar la definición de los contextos indicados previamente, para lo cual diligenciará las tablas anexas al formato de mapa de riesgos identificado con el código GO-FR-005, atendiendo al análisis de los factores relacionados en la tabla No. 2.

5. 1. 2. Identificación de Riesgos por proceso

La identificación de riesgos por proceso desarrolla tres componentes: la definición del riesgo o evento probable que afecta el logro del objetivo del proceso, la identificación de las causas que hacen que se presente el riesgo y las consecuencias que la materialización del riesgo generaría en la Entidad.

- Definición del Riesgo: Para el ejercicio de definir riesgos, los líderes de proceso del Ministerio del Deporte aplicarán los lineamientos de redacción y descripción de riesgos de gestión, corrupción y seguridad digital, establecidos en la guía vigente para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

- Identificación de Causas: consiste en determinar las causas, también conocidas como fuentes o factores de riesgo, esta identificación se realiza a partir del contexto interno, externo y del proceso. Para este análisis, es importante considerar posibles fuentes de información adicionales como resultados de auditoría generados por entes de control interno y/o externo, informes de seguimiento desarrollados por la Oficina de Control Interno de la Entidad, análisis de riesgos materializados en periodos anteriores, PQRSD recibidas y resultados históricos de la gestión institucional, entre otros.

- Identificación de Consecuencias: son los efectos que se generan en la Entidad, a partir de la materialización de los riesgos.

Se resalta que, para la identificación de los riesgos, cada líder de proceso se asegurará de generar sinergia entre los grupos internos de trabajo de sus respectivas Direcciones Técnicas y/o dependencias, para identificar y formular los riesgos del proceso de manera consolidada en un único documento de mapa de riesgos.

5. 1. 2. 1. Identificación Riesgos de Corrupción

Los riesgos de corrupción, entendidos como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, son identificados a partir de la siguiente estructura, si el riesgo identificado cumple con estos cuatro componentes se trata de un riesgo de corrupción:

Acción u omisión + Uso del poder + Desviación de la gestión de lo público + El beneficio privado

Los riesgos de corrupción serán consolidados anualmente por la Oficina Asesora de Planeación una vez sean definidos y remitidos por parte de cada uno de los respectivos líderes de procesos; posterior a la consolidación del mapa de riesgos de corrupción será cargado en la página web de la Entidad, con el propósito de disponer el documento a la ciudadanía, servidores públicos y contratistas para contar con sus apreciaciones y comentarios, previo a la publicación del mapa de riesgos en la página web de conformidad con lo establecido en el literal g) del artículo 9 de la Ley 1712 de 2014.

5. 1. 2. 2. Identificación Riesgos de Gestión y de Seguridad Digital

Para la identificación de riesgos de gestión, se tendrá en cuenta que este se relacione directamente con las características del objetivo del proceso, en caso de no ser así puede corresponder a una causa o una consecuencia y por lo tanto se debe reformular.

En cuanto a la identificación de riesgos de seguridad digital, es de resaltar que estos se basan en la afectación en términos de “integridad”, “confidencialidad” o “disponibilidad” de un activo o un grupo de activos dentro del proceso; por lo tanto, el Ministerio del Deporte gestionará los riesgos asociados a los activos de seguridad digital con nivel de criticidad alta. Para los riesgos de seguridad digital identificados se deben analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

En esta actividad de identificación de riesgos de seguridad digital, es importante tener en cuenta cuáles y cuantos activos de información (Inventario de activos MINDEPORTE) tiene cada proceso. Las amenazas pueden causar daño permanente o temporal a los activos de información, procesos y sistemas de soporte de la Entidad, las más comunes son:

• Incidentes naturales

• Daños físicos

• Humanos

• Interrupción de servicios

• Labores no autorizadas

5. 1. 2. 3. Tipología de Riesgos

El Ministerio del Deporte adopta las tipologías de riesgos descritas en la guía para la administración del riesgo y el diseño de controles en entidades públicas, adicionalmente incluye los riesgos de tipo ambiental, en concordancia con el compromiso de la Alta Dirección frente al cuidado del medio ambiente.

5.2. Valoración de Riesgos

La valoración de riesgos consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial o inherente. La valoración de riesgos se desarrolla a partir de dos elementos, que corresponden al análisis del riesgo y la evaluación de riesgos.

5. 2. 1. Análisis de Riesgos

El análisis de riesgos se realiza sobre las causas, la probabilidad y el impacto de los riesgos.

5. 2. 1. 1. Análisis de Causas

El análisis de causas parte de la identificación de las actividades que mayor aporte generan al cumplimiento de los objetivos, estas actividades son consideradas como críticas o factores clave de éxito, por ende, deben ser tenidas en cuenta para priorizar las causas que generan la materialización de los riesgos. En este sentido, de las causas identificadas, se deberán seleccionar las de mayor relevancia sobre el riesgo analizado, por tal motivo se debe aplicar el método de "Matriz de Priorización" descrito en el Anexo No. 5 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – Versión 4.

Posteriormente, sobre las causas priorizadas, se realizará análisis de causa raíz mediante la aplicación del método de los ¿por qué?, el cual consiste en preguntar ¿por qué? se presenta la situación descrita en la causa priorizada, tantas veces hasta que se detecte la causa raíz del riesgo identificado.

5. 2. 1. 2. Análisis de Probabilidad

La probabilidad entendida como la posibilidad de que ocurra un riesgo, es definida a partir de los siguientes criterios:

• Frecuencia: analizar la cantidad de veces que se ha materializado el riesgo en un periodo de tiempo.

• Factibilidad: analizar la presencia de factores internos y externos que pueden generar el riesgo, son factores que no se han presentado pero que es posible que se den.

Para determinar la probabilidad de ocurrencia en el proceso inicial de formulación de mapas de riesgo en el Ministerio del Deporte, se definirá la probabilidad bajo el criterio de factibilidad, aplicando la siguiente matriz de priorización, atendiendo a las instrucciones descritas en cada campo de la tabla No. 3:

Tabla No. 3. Matriz de priorización de probabilidad bajo el criterio de factibilidad.

No.	Riesgo	Integrante 1	Integrante 2	Integrante 3	Total	Promedio	Nivel
Consecutivo del riesgo	Describir el riesgo al cual se le va a determinar la probabilidad	Cada integrante del equipo que participe en la valoración de los riesgos, deberá estimar el nivel de probabilidad de 1 a 5, donde 1 es rara vez y 5 es casi seguro.			Realizar la sumatoria de los valores estimados por cada integrante del equipo.	Calcular el promedio de los valores estimados por los integrantes del equipo.	Asignar el nivel de probabilidad de acuerdo a la tabla No. 4.
Ejemplo:							
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad.	Se espera que el evento ocurra en la mayoría de las circunstancias. (5)	(4)	(3)	12	4	(4) Probable

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 39.

A partir de la segunda vigencia en que el Ministerio del Deporte gestione los riesgos bajo la metodología adoptada en la presente política y de contar con una línea base frente al número de veces que se hayan presentado los eventos de riesgo; los líderes de proceso generarán la actualización de la probabilidad de ocurrencia de los riesgos bajo el criterio de frecuencia según se presenta en la siguiente tabla:

Tabla No. 4. Criterios para calificar la probabilidad.

Nivel	Descriptor	Descripción	Frecuencia
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las ocasiones en que se desarrolla la actividad crítica asociada al riesgo.	Más de una (1) vez al año.
4	Probable	El viable que el evento ocurra en la mayoría de las ocasiones en que se desarrolla la actividad crítica asociada al riesgo.	Al menos una (1) vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos una (1) vez en los últimos dos (2) años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una (1) vez en los últimos cinco (5) años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos cinco (5) años.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 39.

5. 2. 1. 3. Análisis de Impacto

El impacto se entiende como las consecuencias que pueden generarse en la Entidad a partir de la materialización de un riesgo. El análisis y definición del impacto se realiza a partir de las consecuencias identificadas en la etapa 1.2. Identificación del Riesgo por Proceso, y se establecerá de acuerdo con los criterios relacionados en las siguientes tablas para los riesgos de gestión, seguridad digital y corrupción.

Riesgos de Gestión

En la tabla No. 5 se definen los criterios para la calificación del impacto de riesgos de gestión:

Tabla No. 5. Niveles para la calificación de impacto de riesgos de gestión.

Nivel	Impacto o Consecuencia
Insignificante	• No hay interrupción en la formulación, adopción, dirección, coordinación, inspección, vigilancia, control y ejecución de la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional del Ministerio del Deporte.
Menor	• Se presenta interrupción en la formulación, adopción, dirección, coordinación, inspección, vigilancia, control y ejecución de la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física por algunas horas. • Reclamaciones o quejas de los beneficiarios que implican investigaciones disciplinarias. • Imagen Institucional afectada localmente.
Moderado	• Se presenta interrupción en la formulación, adopción, dirección, coordinación, inspección, vigilancia, control y ejecución de la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física por 1 día. • Reclamaciones o quejas de los usuarios que implican denuncias ante los entes reguladores o demandas para la Entidad. • Inoportunidad de la información, generando retrasos en la atención de los beneficiarios de los programas, planes y proyectos. • Reproceso de actividades. • Imagen Institucional afectada en el orden nacional por retrasos en la prestación de los servicios a nuestros beneficiarios. • Investigaciones penales, fiscales o disciplinarias.
Mayor	• Se presenta interrupción en la formulación, adopción, dirección, coordinación, inspección, vigilancia, control y ejecución de la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física por 2 días. • Perdida de información crítica que puede ser recuperada total o parcialmente • Sanción por parte de los entes de control u organismo regulador • Incumplimiento en las metas y objetivos institucionales y de gobierno • Imagen Institucional afectada en el orden nacional o regional por retrasos en la prestación de los servicios a nuestros beneficiarios.
Catastrófico	• Se presenta interrupción en la formulación, adopción, dirección, coordinación, inspección, vigilancia, control y ejecución de la política pública, planes, programas y proyectos en materia del deporte, la recreación, el aprovechamiento del tiempo libre y la actividad física por 5 días o más. • Intervención por parte de un ente de control u organismo regulador • Perdida de información crítica que no puede ser recuperada • Incumplimiento en las metas y objetivos institucionales y de gobierno afectando de forma grave la ejecución presupuestal • Imagen Institucional afectada en el orden nacional o regional por actos de corrupción comprobados.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 40-41.

Riesgos de Seguridad Digital

En la tabla No. 6 se definen los criterios para la calificación del impacto de riesgos de seguridad digital:

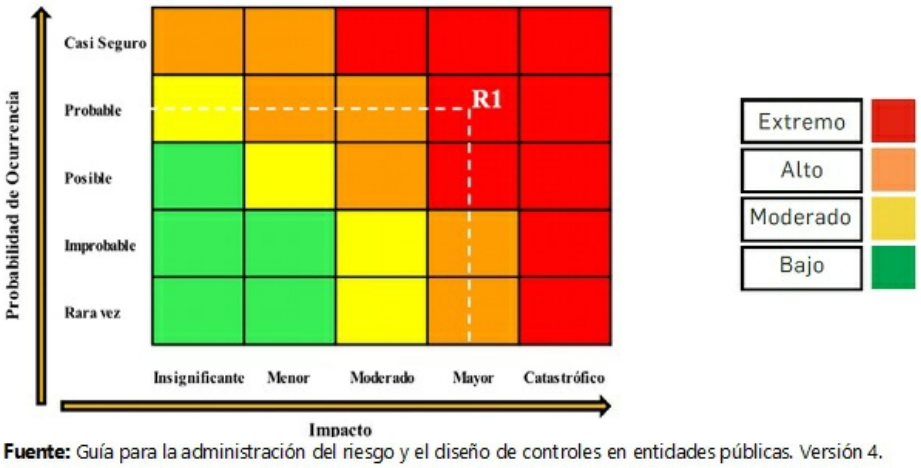
Tabla No. 6. Niveles para la Calificación de Impacto de riesgos de seguridad digital.

Nivel	Impacto o Consecuencia
Insignificante	• Sin afectación a la integridad • Sin afectación de la disponibilidad • Sin afectación de la confidencialidad
Menor	• Afectación leve a la integridad • Afectación leve de la disponibilidad • Afectación leve de la confidencialidad
Moderado	• Afectación moderada a la integridad de la información debido al interés particular de los colaboradores y terceros. • Afectación moderada de la disponibilidad debido al interés particular de los colaboradores y terceros • Afectación moderada de la confidencialidad debido al interés particular de los colaboradores y terceros.
Mayor	• Afectación grave a la integridad de la información debido al interés particular de los colaboradores y terceros. • Afectación grave de la disponibilidad debido al interés particular de los colaboradores y terceros • Afectación grave de la confidencialidad debido al interés particular de los colaboradores y terceros.
Catastrófico	• Afectación muy grave a la integridad de la información debido al interés particular de los colaboradores y terceros. • Afectación muy grave de la disponibilidad debido al interés particular de los colaboradores y terceros • Afectación muy grave de la confidencialidad debido al interés particular de los colaboradores y terceros.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 42-43.

Una vez definidos los niveles de probabilidad e impacto para los riesgos de gestión y seguridad digital, se deben ubicar los correspondientes niveles en el mapa de calor (Imagen No. 3) para identificar la zona de riesgo inherente.

Imagen No. 3. Mapa de Calor - Zonas de Riesgo.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

Riesgos de Corrupción

La calificación del impacto de riesgos de corrupción, se deberá realizar mediante respuesta a las preguntas establecidas en la tabla No. 7, con el fin de determinar el impacto del riesgo si se llegase a materializar.

Tabla No. 7. Criterios para la calificación de Impacto en riesgos de corrupción.

N °	Pregunta: Si el riesgo de corrupción se materializa podría...	Respuesta Si	Respuesta No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.	**Total**		
Moderado	Genera medianas consecuencias sobre la Entidad		
Mayor	Genera altas consecuencias sobre la Entidad.		
Catastrófico	Genera consecuencias desastrosas para la Entidad		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 46.

De acuerdo con la tabla anterior, el impacto de riesgos de corrupción se clasificará teniendo en cuenta únicamente los niveles de "moderado", "mayor" y "catastrófico", considerando que este tipo de riesgos siempre serán significativos para el Ministerio del Deporte; es así que los niveles de impacto "insignificante" y "menor" no aplican para establecer este tipo de riesgos.

5. 2. 2. Evaluación de Riesgos

La etapa de evaluación de riesgos propende por facilitar la toma de decisiones para la administración de riesgos, a partir del análisis de la identificación del riesgo inherente y la valoración del diseño y la ejecución de los controles establecidos para mitigar las causas que dan origen a la materialización de riesgos.

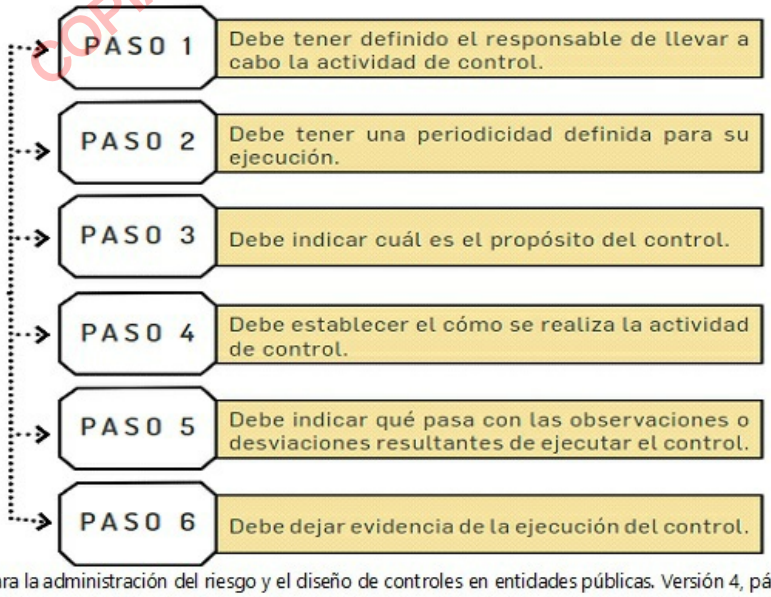
5. 2. 2. 1. Análisis Riesgo Inherente y Diseño de Controles

El riesgo inherente es el riesgo ante el cual se expone la Entidad, antes de aplicar controles. Para estos riesgos inherentes, es importante verificar que cumplan con las siguientes características, previo al diseño de los controles:

- Los riesgos identificados deben tener relación con los objetivos institucionales y del proceso.
- Las causas identificadas sean factores que dan origen a la materialización del riesgo.
- Cada causa identificada deberá tener al menos un control asociado, sin embargo, se pueden diseñar controles eficientes que permitan mitigar más de una causa.
- Las causas se deben trabajar de manera separada en el mapa de riesgos por proceso.

Los líderes de proceso, quienes representan la primera línea de defensa en la administración del riesgo, diseñarán controles a los riesgos inherentes. Para el adecuado diseño de los controles se deberán desarrollar y registrar en los mapas de riesgo de cada proceso, la totalidad de los pasos relacionados en la imagen 4; con el fin de evitar debilidades en el diseño de controles.

Imagen No. 4. Pasos para el diseño de controles.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 49.

5. 2. 2. 2. Valoración de Controles

La valoración de controles se realiza en el marco del diseño de los controles y la ejecución de los mismos; lo anterior, considerando que un diseño adecuado por sí solo no garantiza la mitigación del riesgo, por ende, para lograr este propósito se deben ejecutar los controles de acuerdo con las variables bajo los cuales se diseñaron.

La evaluación de los controles se desarrollará bajo los lineamientos y criterios establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas vigente.

5. 2. 2. 3. Riesgo Residual

Producto de la aplicación de controles sobre los riesgos inherentes, se genera un desplazamiento en términos de probabilidad e impacto del riesgo en el mapa de calor que define las zonas de riesgos; esta nueva ubicación denota el nivel de riesgo residual (Tabla No. 8).

Tabla No. 8. Desplazamientos de la probabilidad e impacto de los riesgos.

Solidez del Conjunto de Controles	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir el impacto	# Columnas en el mapa de calor que desplaza en el eje de la probabilidad	# Columnas en el mapa de calor que desplaza en el eje de impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4, pág. 66.

5. 2. 2. 4. Tratamiento y manejo de riesgos

Las respuestas que se pueden dar en el tratamiento de los riesgos de la Entidad son las siguientes:

- **Aceptar el riesgo:** si el riesgo cumple con los niveles de aceptación del riesgo establecidos en el numeral 4 del presente documento, no será necesario establecer controles y el riesgo se acepta por parte de la Entidad por lo tanto no se adopta ninguna medida.

- **Evitar el riesgo:** Cuando se identifique un escenario de riesgos extremo en el Ministerio del Deporte podrá eliminar la actividad o actividades que garanticen la eliminación del riesgo evitando su materialización.

- **Compartir el riesgo:** Cuando el Ministerio del Deporte por sus propios medios no pueda reducir a niveles aceptables el riesgo, este podrá ser compartido con una parte interesada que pueda gestionarlo con más eficacia, lo cual no implica que se traslade la responsabilidad del riesgo.

- **Reducir el Riesgo:** Cuando el Ministerio del Deporte por sus propios medios pueda establecer controles que al ser correctamente aplicados permitan llevar el riesgo a un nivel residual aceptable para la Entidad, estos controles deben atacar la probabilidad o el impacto según sea conveniente.

  Para propender por el logro de los objetivos institucionales y gubernamentales, los controles se deben orientar a detectar y prevenir la materialización de los riesgos. Por lo anterior, le corresponde a la primera línea de defensa (líderes de proceso) el establecimiento de sus actividades de control y garantizar que estas se desplieguen a través de los procedimientos documentados de sus respectivos procesos.

Acciones a implementar en caso de materialización de un riesgo

En el evento que se presente materialización de un riesgo y con relación a las responsabilidades de la primera línea de defensa, es decir, los directores, líderes de proceso de la Entidad, deberán desarrollar las siguientes acciones tendientes a la mitigación del impacto sobre los objetivos institucionales:

Tabla No. 9. Acciones en caso de materialización de Riesgos.<>/center

Tipo de Riesgo Materializado	Acciones a Tomar
Corrupción	• Ejecutar de inmediato las acciones definidas en el plan de tratamiento del riesgo, que permitan mitigar el impacto sobre los objetivos institucionales por su materialización. • Una vez sea detectada la materialización del riesgo, debe ser reportada a la Oficina Asesora de Planeación e informar a las autoridades competentes la ocurrencia del hecho de corrupción. • En el reporte de la materialización se debe realizar una descripción detallada de lo ocurrido, en la cual se identifique(n) la(s) causa(s) que originaron la materialización del riesgo, así como el impacto generado al proceso. Esta descripción será presentada una vez sea detectada la materialización del riesgo y adicionalmente el reporte se debe ver reflejado en el monitoreo periódico cuatrimestral definido en la presente política. • Revisar el mapa de riesgos, con el fin de fortalecer la identificación de causas de los riesgos y el diseño de los controles. • Verificar la implementación de las acciones de control definidas en el mapa de riesgos. • De acuerdo al análisis de la materialización del riesgo, actualizar el mapa de riesgos, teniendo en cuenta que la materialización afecta la probabilidad y/o impacto en la valoración del riesgo.
De gestión y Seguridad Digital	• Reportar la materialización del riesgo a la Oficina Asesora de Planeación, en la cual se realice una descripción detallada de lo ocurrido, identificando la(s) causa(s) que generaron la materialización del riesgo y el impacto generado al proceso. Esta descripción será presentada en el monitoreo periódico cuatrimestral definido en la presente política. • Ejecutar de inmediato las acciones definidas en el plan de tratamiento del riesgo, que permitan mitigar el impacto sobre los objetivos institucionales por su materialización. • Revisar el mapa de riesgos, con el fin de fortalecer la identificación de causas de los riesgos y el diseño de los controles. • De acuerdo al análisis de la materialización del riesgo, actualizar el mapa de riesgos, teniendo en cuenta que la materialización afecta la probabilidad y/o impacto en la valoración del riesgo.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

5. 2. 3. Monitoreo y Revisión

Para el monitoreo y revisión de la administración del riesgo, el Ministerio del Deporte adopta el esquema de líneas de defensa que desarrolla el Modelo Estándar de Control Interno – MECI, en el cual se establecen los roles y responsabilidades así:

Línea Estratégica

Corresponde a la Alta Dirección y el Comité Institucional de Coordinación de Control Interno, cuya función principal es definir el marco general para la administración del riesgo y la supervisión de su cumplimiento. Asimismo, cumple con:

- Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.

- Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.

- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.

- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.

- Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la Entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

Primera Línea de Defensa

Corresponde a los gerentes públicos y líderes de procesos, de la Entidad, quienes deben asegurarse que la presente política se implemente con el fin de mitigar los riesgos en la operación; reportando a la segunda línea de defensa los seguimientos, avances y dificultades encontradas. La primera línea de defensa tiene a cargo la responsabilidad de:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.

- Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos de sus procesos.

- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

- Revisar y reportar a la Oficina Asesora de Planeación, los eventos de riesgos que se han materializado en la Entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.

- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

Segunda Línea de Defensa

Está conformada por la Oficina Asesora de Planeación como líder que soporta y guía a la línea estratégica y a la primera línea de defensa en la administración de los riesgos; de igual manera hacen parte de la segunda línea de defensa los coordinadores de otros sistemas de gestión, área financiera y de TIC's, contratación y gestión documental, dado que responden y evalúan de manera transversal los temas correspondientes a estas áreas y son quienes generan información para el aseguramiento de la operación de la Entidad. Como responsabilidades de la segunda línea se encuentran:

- Asesorar la línea estratégica y primera línea de defensa para la implementación y desarrollo de la administración de riesgos.

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de los mapas de riesgos.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- Revisar el adecuado diseño de los controles para la mitigación de los riesgos de los procesos, establecidos por parte de la primera línea de defensa; y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado, y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la Entidad.

- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

- Presentar informes consolidados a la línea estratégica en temas clave de la administración del riesgo y su impacto frente al logro de los objetivos.

- Llevar a cabo un monitoreo independiente al cumplimiento de las etapas de la administración del riesgo y generar reportes que permitan incorporar mejoras, tanto a los riesgos identificados como a los controles aplicados.

- Difundir y asesorar la metodología descrita en la presente política, así como los planes de tratamiento de riesgos identificados en todos los niveles de la Entidad, de tal forma que se asegure su implementación.

- Consolidar y presentar el mapa de riesgos institucional ante el Comité Institucional de Coordinación de Control Interno para su respectivo análisis y retroalimentación.

Tercera Línea de Defensa

Está conformada por la Oficina de Control Interno, le corresponde realizar la evaluación independiente y objetiva sobre la efectividad del sistema de gestión del riesgo, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han

servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.

- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos de los procesos, establecidos por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la Entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.

- Revisar que las acciones de control definidas para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

- Presentar al Comité Institucional de Coordinación de Control Interno los resultados de la evaluación efectuada a la operación de la primera y segunda línea de defensa que incorpore las debilidades, riesgos y oportunidades de mejora .

- Brindar asesoría y acompañamiento técnico y de evaluación y seguimiento a los diferentes pasos de la gestión del riesgo .

- Evaluar la efectividad de la Gestión del Riesgo en la Entidad, así como la adecuada aplicación de controles, planes de contingencia y actividades de monitoreo vinculados a riesgos clave en la Entidad.

- Le corresponde a la Oficina de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la Entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

Responsable de Seguridad Digital

El responsable de la Seguridad digital y de la seguridad de la información del Ministerio del Deporte deberá cumplir las siguientes funciones relacionadas con la gestión del riesgo de seguridad digital:

- Definir el procedimiento para la identificación y valoración de activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, análisis, evaluación y tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgos definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

El reporte del monitoreo y revisión de riesgos de gestión, corrupción y seguridad digital en el Ministerio del Deporte se realizará cuatrimestralmente durante cada vigencia fiscal, para esto, cada líder de proceso deberá consolidar la información relacionada con el plan de tratamiento de los riesgos establecidos en los respectivos mapas de riesgos y remitirlo a la Oficina Asesora de Planeación a más tardar el segundo día hábil anterior al día de corte del cuatrimestre a reportar; lo anterior, con el fin de que la Oficina Asesora de Planeación ejerza su responsabilidad de monitoreo como segunda línea de defensa en la administración del riesgo. No obstante, se requiere que los líderes de proceso ejecuten seguimiento constante a la gestión del riesgo y a la efectividad de los controles, en especial de los riesgos de corrupción.

5. 2. 4. Seguimiento a Riesgos

El seguimiento a riesgos de gestión, corrupción y seguridad digital será adelantado por la Oficina de Control Interno del Ministerio del Deporte de la siguiente manera:

Riesgos de Gestión y Seguridad Digital

A partir del reporte del monitoreo efectuado por cada uno de los líderes de proceso y una vez la Oficina Asesora de Planeación ejecute el respectivo monitoreo a los riesgos, el tercer día hábil siguiente al día de corte del cuatrimestre, procederá a enviar los mapas de riesgo y las evidencias de la aplicación de los controles, a la Oficina de Control Interno, para el respectivo seguimiento a los mapas de riesgo de gestión por proceso.

Riesgos de Corrupción

Para tener un control efectivo sobre los riesgos en especial los de corrupción se realizarán tres seguimientos por parte de la Oficina de Control Interno, en los cuales se verificará la efectividad de los controles:

- Primer seguimiento: Con corte a 30 de abril.

- Segundo seguimiento: Con corte a 31 de agosto.

- Tercer seguimiento: Con corte al 31 de diciembre.

Los resultados de los seguimientos serán publicados en la página web de la Entidad y en el Sistema de Gestión Institucional, dentro de los diez (10) primeros días de los meses de mayo, septiembre y enero.

A partir de los resultados de seguimiento a mapas de riesgos, presentados por la Oficina de Control Interno y en el marco de la mejora, los líderes de proceso deberán formular las acciones correctivas y de mejoramiento a que haya lugar, para el fortalecimiento de la administración del riesgo en la Entidad.

5.3. Comunicación y Consulta

La política de administración del riesgo del Ministerio del Deporte, será socializada a cada una de las dependencias de la Entidad. La etapa de implementación de la política al interior de los procesos, deberá ser mediante acciones participativas en las que se involucren los servidores que por su conocimiento y experiencia puedan aportar en la identificación y valoración de riesgos. Así mismo, la política y el mapa de riesgos de corrupción serán publicados en la plataforma del Sistema de Gestión Institucional y la página web de la Entidad, con el propósito de que sea de conocimiento de todas las partes interesadas.

6. REFERENCIAS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas riesgos de gestión, corrupción y seguridad digital
- Guía Técnica Colombiana GTC 137
- Norma Técnica Colombiana NTC – ISO 31000
- Norma ISO 27001:2005
- Anexo 4 – Lineamientos para la gestión de riesgos de Seguridad Digital en Entidades Públicas

Acta de Aprobación Política de Administración del Riesgo en Comité Institucional de Coordinación de Control Interno

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	03/Mar/2016	Creación del documento.
2	14/Feb/2017	• Se realiza la revisión general de la política. • Ajuste al numeral 6.3 Riesgos de Corrupción. • Se incluyen numerales: 9 Referencias 10 Control de cambios Aprobación del documento
3	04/Dic/2019	Se ajusta la política de administración del riesgo, de acuerdo a los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.
3	04/Dic/2019	El cargue de esta Política en el sistema fue realizado posterior a la fecha de aprobación dado que el aplicativo ISOLUCION fue restablecido el 25 de Octubre del año 2019,
4	26/May/2020	Se realizaron los siguientes ajustes: • En el objetivo se detallan los principios para la administración del riesgo. • En el glosario se aclara la definición de compartir el riesgo • En los niveles de aceptación se aclaró que el monitoreo para todos los riesgos ubicados en zonas moderada, alta y extrema es constante y se debe generar reportes cuatrimestrales. • En establecimiento del contexto se ajustó la denominación de activos de seguridad digital y se actualizaron las variables que incluye el inventario de los activos de seguridad digital. • En el componente de identificación de riesgos de gestión y seguridad digital, se estableció que la Entidad gestionará los riesgos de seguridad digital asociados a los activos con criticidad alta. • En la tabla de criterios para calificar la probabilidad se ajustaron las frecuencias de acuerdo con las establecidas en la guía de riesgos del DAFP. • En la tabla de criterios para calificar el impacto en riesgos de gestión, se incluyeron las acciones de formulación, adopción, dirección, coordinación, inspección, vigilancia y control en el primer criterio de cada nivel. • En monitoreo y revisión se incluyen las funciones del responsable de la seguridad digital en la Entidad y se ajusta periodicidad para la entrega de los monitoreos por parte de los líderes de proceso. • En referencias se incluye el Anexo 4 - Lineamientos para la gestión de riesgos de Seguridad Digital en Entidades Públicas.

ELABORÓ	REVISÓ	APROBÓ
		Nombre: Diana Carolina Breton Franco.

Nombre: Juan Sebastian Vega Lagos
Cargo: Sistema de Gestión de Calidad
Fecha: 27/May/2020

Nombre: Kelly Alexandra Mariño Estupiñan
Cargo: Profesional Especializado - Planeación
Fecha: 27/May/2020

Nombre: Monica Monsalvo Torres
Cargo: Jefe Oficina Asesora de Planeación
Fecha: 27/May/2020

Cargo: Director Fomento y Desarrollo
Fecha: 29/May/2020

Nombre: Miguel Ernesto Acevedo Rico
Cargo: Director Posicionamiento y Liderazgo Deportivo
Fecha: 02/Jun/2020

Nombre: Diego German Montero Osorio
Cargo: Director Recursos y Herramientas del Sistema
Fecha: 02/Jun/2020

Nombre: Viviana Forero Alvarez
Cargo: Director Inspección Vigilancia y Control
Fecha: 02/Jun/2020

Nombre: Jaime Arturo Guerra Rodriguez
Cargo: Secretario General
Fecha: 02/Jun/2020

Nombre: Maria Carmenza Valverde Pineda
Cargo: Jefe Oficina Asesora Jurídica
Fecha: 02/Jun/2020

Nombre: Lina maria Barrera Rueda
Cargo: Viceministro(a)
Fecha: 03/Jun/2020

Nombre: Ernesto Lucena Barrero
Cargo: Director
Fecha: 03/Jun/2020