PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2026

MINISTERIO DEL DEPORTE

GRUPO INTERNO DE TRABAJO TIC´S

VERSIÓN 7

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio del Deporte, define la estrategia, actividades y acciones para mitigar los riesgos y mantener su valoración en un residual aceptable para el Ministerio y busca fomentar una cultura preventiva que permita la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos asociados a la seguridad y privacidad de la información, seguridad digital y la continuidad operativa de los servicios tecnológicos.

El Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) en las entidades del estado tiene como objetivos:

- Generar confianza en el ciudadano
- Ayuda a cumplir la misión y la visión de la entidad
- Proteger la relación del estado con sus usuarios
- Implementar procesos de mejora permanente

Basados en estos objetivos fundamentales, se busca que la entidad asegure los procesos y los ejecute de manera más eficiente a través del proceso de mejora continua. Para ello, el Ministerio del Deporte cuenta con la Resolución No. 002020 del 23 de diciembre de 2021 por la cual se aprueba y adopta el Sistema de Gestión de Seguridad de la Información (SGSI), la cual se desarrolla en base en tres pilares fundamentales: Confidencialidad, Integridad y Disponibilidad.

2. OBJETIVO

Establecer lineamientos claros para gestionar los riesgos asociados a seguridad y privacidad de la información, seguridad digital y continuidad operativa de los servicios en el marco de la misión del Ministerio, que garantice la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

OBJETIVOS ESPECIFICOS:

- Identificar y actualizar los riesgos de seguridad de la información del Ministerio.

- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en los procesos de la Entidad.

- Proponer e implementar controles que apunten a minimizar la probabilidad de ocurrencia de los riesgos identificados.

- Sensibilizar y capacitar a los funcionarios y contratistas en buenas prácticas de ciberseguridad, promoviendo una cultura institucional de seguridad de la información.

- Apoyar a las diferentes áreas de la entidad en el desarrollo del Sistema de Gestión de Seguridad y Privacidad de la Información.

3. ALCANCE

El Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2026, abarca a todos los funcionarios, contratistas y terceros que interactúan con los activos de información del Ministerio del Deporte, se enfoca en identificar, valorar, evaluar y tratar los riesgos de seguridad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado, a los que se les definirá un plan de acción con actividades que fortalezcan los controles definidos para mantener dichos niveles, acorde con los lineamientos definidos por el Ministerio.

4. DEFINICIONES

- **Activo de Información:** Es todo bien, documento o servicio que la entidad considera importante tales como: documentos físicos y electrónicos, software, bases de datos, sistemas de información, hardware, equipos de comunicaciones y cargos.
- **Amenaza:** Causa potencial de un incidente no deseado, es un escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o

impacto negativo en la institución (materializar el riesgo).

- **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.
- **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.
- **Control o Medida:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable ante la demanda de una entidad autorizada.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de la información de ser precisa y completa.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de Seguridad de la Información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. ESTRATEGIA DE DESARROLLO DEL PLAN

El objetivo del plan de tratamiento de riesgos de seguridad y privacidad de la información del año 2025 consistió en relacionar la Política de Administración de Riesgos, la Política de Protección de Datos Personales, el Plan de Seguridad y Privacidad de la Información y los riesgos y acciones de control identificados en los mapas de riesgos definidos en cada uno de los procesos de la entidad de acuerdo con el documento de inventario de activos.

De acuerdo con estos objetivos se realiza el siguiente seguimiento al Plan durante la vigencia 2025:

Resumen avance de seguimiento Noviembre 2025

Deporte	Noviembre
Seguimiento plan de tratamiento de Riesgos de seguridad y Privacidad de la Información	
POLÍTICA DE ADMINISTRACIÓN DE RIESGO	80
POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	100
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	71
INVENTARIO ACTIVOS DE INFORMACIÓN	100
CALIFICACIÓN AVANCE NOVIEMBRE 2025	**87,75**

El Plan de Tratamiento de Riesgos de Seguridad de la Información vigencia 2026

Está basado en las directrices de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 7, emitido por el Departamento Administrativo de Función Pública y en la Política de Administración del Riesgo del Ministerio del Deporte Versión 2025.

La etapa de implementación se centra en la ejecución y cumplimiento de las actividades y objetivos planteados, teniendo en cuenta los roles y responsabilidades y los tiempos establecidos por la Entidad en la Política de Administración del Riesgo.

Es un proceso cíclico que busca identificar los riesgos, vulnerabilidades, causas, amenazas, impacto, consecuencias, controles y el tratamiento según aplique para cada riesgo analizado y evaluado.

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Revisión y/o actualización del Mapa de Riesgos de Seguridad de la Información	Líder de Seguridad	Tercera semana- Enero 2026	Cuarta semana Marzo 2026	Identificar, analizar, actualizar y evaluar los riesgos de Seguridad de la Información
Revisión y/o actualización de planes de tratamiento de riesgos de Seguridad	Líder de Seguridad / Líderes de Procesos	Cuarta semana Enero 2026	Cuarta semana Marzo 2026	Identificar, analizar, actualizar y evaluar los planes de tratamiento de riesgos de Seguridad de la Información.
Revisión y/o actualización de indicadores de medición; Clave del riesgo / Desempeño del control	Líder de Seguridad / Líderes de Procesos	Cuarta semana Enero 2026	Cuarta semana Marzo 2026	Analizar, crear o actualizar indicadores que permitan evaluar la eficacia de los controles (uno por cada control definido).
Aprobación de Mapa de Riesgos	Oficina de planeación	Primera semana Marzo 2026	Cuarta semana Marzo 2026	Aprobación del Mapa y Plan de tratamiento de riesgos de seguridad de la información.
Seguimiento planes de tratamiento	Líder de Seguridad / Líderes de Procesos	Primera semana Abril 2026	Cuarta semana Abril 2026	Realizar seguimiento a los planes de tratamiento de riesgos de seguridad de la información de los diferentes procesos.
Implementación de controles	Líder de Seguridad	Cuarta semana Enero 2026	Seguimiento cuatrimestral	Diseñar controles para mitigar riesgos identificados, seguimiento del plan y avance en la disminución de la probabilidad de materialización del riesgo.
Seguimiento Mapa de Riesgos	Líder de Seguridad	Cuarta semana Abril	Seguimiento cuatrimestral	Emitir informes cuatrimestrales de seguimiento a riesgos con las respectivas evidencias.

6. RECURSOS

El Ministerio dispondrá de los siguientes recursos para gestionar los riesgos de seguridad de la información.

RECURSOS	DESCRIPCIÓN
Humanos	• El Líder de Seguridad de la Información es responsable de liderar, definir e implementar políticas y lineamientos de seguridad de la información, estableciendo estrategias y procedimientos que contribuyan a la mejora continua de la seguridad y privacidad de la información. • Los responsables de los procesos y dependencias deben designar el personal idóneo y necesario para la identificación y gestión de riesgos de seguridad de la información.
Técnicos	• Política de administración del riesgo del Ministerio del Deporte • Herramienta para la gestión de riesgos
Logísticos	• Recursos y logística para la transferencia de conocimiento, socializaciones y seguimiento a la gestión de riesgos.
Financieros	• Recursos asignados a Seguridad de la Información en la vigencia presupuestal del 2026.

7. MARCO NORMATIVO

Directiva Presidencial 02: Febrero 24 de 2022, “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”.

Decreto 338: Marzo 8 de 2022, "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".

Resolución 746: Marzo 11 de 2022, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

Decreto 767: Mayo 16 de 2022, “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Directiva Presidencial 03: Marzo 15 de 2021, “Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos”.

Resolución 500: Marzo 10 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Conpes 3995: Julio 1 de 2020, Política Nacional de Confianza y Seguridad Digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”.

Resolución 1519: Agosto 24 de 2020, “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

Guía para la administración del riesgo y el diseño de controles en entidades públicas -V7: Agosto 2025, “Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.

Decreto 612: Abril 4 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.

Decreto 1008: Junio 14 de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del

Decreto número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Ley 1915: Julio 12 de 2018, "Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos".

Ley 1712: Marzo 06 de 2014, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decreto 886: Mayo 13 de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

Decreto 1377: Junio 23 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

Ley 1581: Octubre 17 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013".

Ley 1273: Enero 05 de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

8. REFERENCIAS

- Política de Administración del Riesgo, DE-PO-001 versión 3. Oficina Asesora de Planeación - Ministerio del Deporte. Abril de 2024.
- Procedimiento de Administración del Riesgo, DE-PD-011 versión 3. Oficina Asesora de Planeación - Ministerio del Deporte. Julio de 2025.
- Plan de Seguridad y Privacidad de la Información del Ministerio del Deporte, versión 5. Grupo Interno de Trabajo TIC´s. - Ministerio del Deporte. Noviembre de 2025.

9. CONTROL DE CAMBIOS

Versión	Motivo	Responsable	Fecha
1	Creación del documento	Coordinador TIC's	Enero de 2019
2	Actualización del documento	Coordinador TIC's	Diciembre de 2020
3	Actualización del documento	Coordinador TIC's	Enero de 2022
4	Actualización del documento	Coordinador TIC's	Enero de 2023
5	Actualización del documento	Coordinador TIC's	Enero de 2024
6	Actualización del documento	Coordinador TIC's	Marzo de 2025
7	Actualización del documento	Coordinador TIC's	Noviembre de 2025

Elaboró:

Bernardo Angel Rios Santana
Especialista Ciberseguridad

Reviso:

Oscar Ramírez Gómez
Profesional Especializado GIT TIC´S

Aprobó:

Rene Mauricio Pinto Pedraza
Coordinador GIT TIC´s