PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2026

MINISTERIO DEL DEPORTE

GRUPO INTERNO DE TRABAJO TIC´S

VERSIÓN 5

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento tiene como propósito fundamental garantizar la resiliencia de los sistemas de información del Ministerio del Deporte, fortaleciendo la protección de los activos de información y alineándose con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, así como con estándares reconocidos como la ISO/IEC 27001:2022

Este Plan de Seguridad consolida un enfoque basado en la mejora continua, apoyado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Este enfoque prioriza la identificación de riesgos, la implementación de controles efectivos y la promoción de una cultura organizacional de seguridad.

De manera complementaria, el Modelo de Seguridad y Privacidad de la Información (MSPI) establece cinco fases, las cuales son: Diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua. La fase de diagnóstico establece que se debe verificar el estado actual de la entidad, identificar el nivel de madurez y hacer el levantamiento de información requerido; como resultado de esta fase se establece la *Línea Base de Seguridad de la Información*.

2. OBJETIVO

Establecer el Plan de Seguridad y Privacidad de la Información del Ministerio del Deporte 2026, mediante actividades de control que permitan definir, implementar, monitorear, y revisar continuamente del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio del Deporte, las cuales están alineadas con el marco de referencia ISO/IEC 27001:2022, con el fin de garantizar la protección integral de los activos de información, mitigar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información para la vigencia 2026, abarca todos los procesos, activos, personas y sistemas que intervienen en la gestión, uso y protección de la información institucional y aplica a todos los funcionarios, contratistas y terceros que interactúan con los activos de información de la entidad.
Su alcance comprende la ejecución de acciones, tendientes a mejorar aspectos identificados en la línea base de seguridad de la información que establece la gestión de la entidad en 4 dominios de acuerdo con la norma ISO/IEC 27001:2022, dentro de la implementación del MSPI. Este plan asegura el cumplimiento de las normativas vigentes y fomenta una cultura organizacional orientada hacia la seguridad digital.

4. ESTADO ACTUAL

Durante la vigencia 2025, el Ministerio del Deporte implementó diversas estrategias alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), gestionando los controles de los 14 dominios de la norma ISO/IEC 27001:2013 y a partir de agosto 2025 utilizando "el instrumento o herramienta de evaluación MSPI" bajo la ISO/IEC 27001:2022, se está gestiononando la fase I de Autodiagnóstico, identificando controles y brechas, recopilando los soportes documentales que demuestran el cumplimiento de cada control, y formulando actividades para la mejora continua en la implementación del MSPI.

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 a corte del 30 de noviembre de 2025 es del 71 % de Cumplimiento.

A continuación, se muestra el resultado de la implementación de los controles evaluados en el MSPI al corte de noviembre de 2025:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	94	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	100	REPETIBLE
A.8	GESTION DE ACTIVOS	98	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	68	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	68	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	40	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	70	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	76	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	75	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	72	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		71,00	100	GESTIONADO

5. DETALLE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

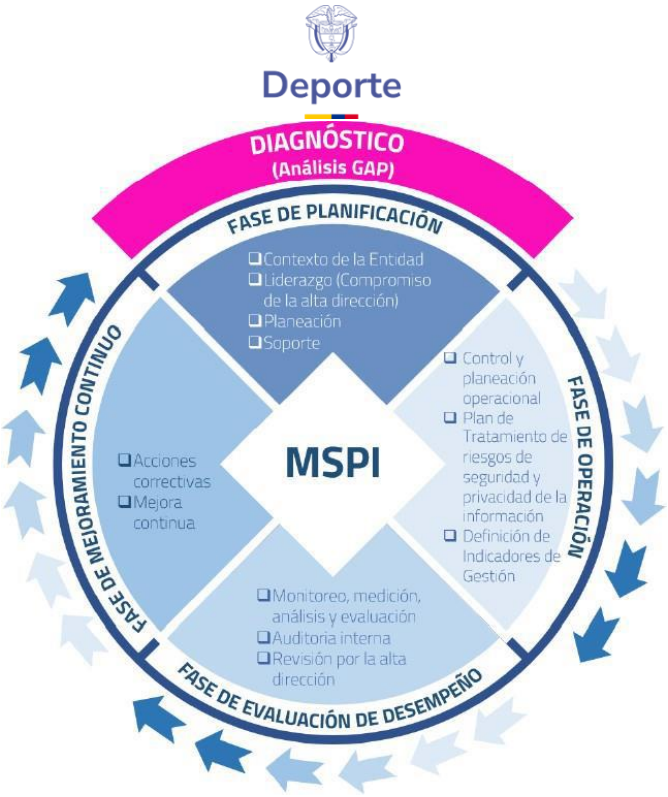


Ilustración 1. Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.

El Plan de Seguridad y Privacidad de la Información bajo la norma ISO/IEC 27001:2022 comprende los siguientes 4 Dominios con 94 controles, con sus respectivas actividades, tareas y responsables:

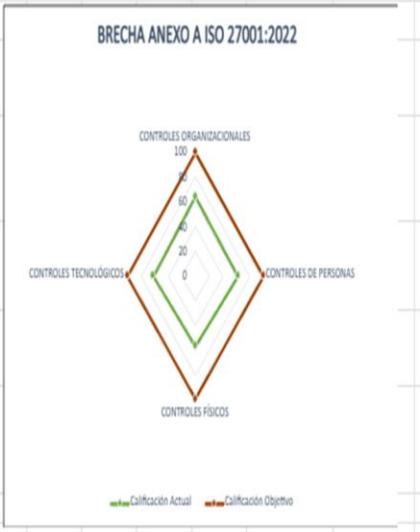
1. Personas
2. Físicos
3. Organizacionales
4. Tecnológicos.

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022 a corte del 30 de noviembre de 2025 es del 62 % de Cumplimiento.

A continuación, se muestra el resultado del Autodiagnóstico de los controles evaluados en el MSPI al corte de noviembre de 2025:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	64	100	GESTIONADO
A.6	CONTROLES DE PERSONAS	63	100	GESTIONADO
A.7	CONTROLES FÍSICOS	57	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	62	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		62	100	GESTIONADO



El plan de trabajo diseñado para ser revisado y aprobado tanto por la Coordinación de Tecnologías de la Información y las Comunicaciones (GIT TIC´S), como por el Comité de Gestión y Desempeño es el siguiente:

GESTIÓN DE ACTIVOS DE INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información 2026 establece que la gestión de activos de información debe ser un proceso continuo que incluya la identificación, clasificación, actualización y protección de los activos tecnológicos, físicos y de información.

Actualización cronograma de actividades- Matriz de activos de información

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Capacitación sobre la matriz de activos de información	Líder de Seguridad	Tercera semana Enero 2026	Cuarta semana- Enero 2026	Capacitar a los responsables en el uso de la matriz y en los principios básicos de activos de información.
Registro de la matriz de activos	Responsables de cada dependencia	Segunda semana- Febrero 2026	Tercera semana- Marzo 2026	Identificar y clasificar activos de información según los procesos de cada área

Revisión de información enviada por las dependencias	Líder de Seguridad	Cuarta semana-Marzo 2026	Primera semana-Abril 2026	Revisar documentación enviada por las dependencias (responsables) , unificar información y establecer retroalimentación y mejora continua.
Ajustes y envío de retroalimentación a dependencias	Líder de Seguridad	Primera Semana-Abril 2026	Segunda Semana-Abril 2026	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada	Responsables de cada dependencia	Segunda Semana-Abril 2026	Cuarta semana-Abril 2026	Información debidamente ajustada y completada.
Validación priorización de activos críticos	Líder de Seguridad	Cuarta semana-Abril 2026	Segunda semana-Mayo 2026	Revisar, validar y priorizar los activos críticos según el impacto al negocio y continuidad al mismo.
Integración con el SGSI	Oficina de planeación	Segunda semana Mayo 2026	Cuarta semana-Mayo 2026	Incorporar los activos priorizados en el SGSI y actualizar los controles.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es un componente esencial del Plan de Seguridad y Privacidad de la Información 2026, ya que permite identificar, evaluar y mitigar las amenazas que podrían comprometer la confidencialidad, integridad, disponibilidad y privacidad de los activos críticos del Ministerio del Deporte.

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.

GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio desarrollará, actualizará y gestionará sus políticas y procedimientos de seguridad de la información con base en las siguientes directrices:

Ciclo de revisión de las políticas: Establecer un ciclo de revisión que incluya la creación, aprobación, difusión, implementación, monitoreo y actualización de las políticas. Cada política debe estar alineada con las normativas aplicables y revisarse al menos una vez al año.

Capacitación continua: Garantizar que los responsables, funcionarios y contratistas

comprendan las políticas y procedimientos mediante sesiones de formación, con especial atención a aquellas áreas que interactúan directamente con activos críticos.

Monitoreo de cumplimiento: Realizar auditorías regulares para evaluar la adherencia a las políticas y su efectividad en la mitigación de riesgos.

Adaptabilidad y mejora continua: Ajustar las políticas y procedimientos en respuesta a cambios regulatorios, tecnológicos y operativos, asegurando que sigan siendo pertinentes y efectivas.

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Revisión de políticas y procedimientos de seguridad	Líder de Seguridad / Profesionales Especializados GIT TICS	Tercera semana-Enero 2026	Cuarta semana-Febrero 2026	Entrega de procedimientos y políticas vigentes 2025 para revisión por parte del grupo GIT TICS.
Capacitación de procedimientos y de políticas de seguridad	Líder de Seguridad	Primera semana-Marzo 2026	Cuarta semana-Junio 2026	Socializar los cambios y formar a los funcionarios y contratistas para su cumplimiento.
Monitoreo de cumplimiento	Líder de Seguridad	Seguimiento trimestral	Seguimiento cuatrimestral	Auditorías internas para verificar la adherencia y la efectividad de las políticas.
Revisión anual	Líder de Seguridad	Tercera semana-Enero 2026	Primera semana-Diciembre 2026	Evaluar el estado general de las políticas y procedimientos para preparar el ciclo 2027.

PLANIFICACIÓN – Toma de conciencia y comunicación

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Conciencia y comunicación	Líder de Seguridad	Enero 2026	Febrero 2026	Elaborar matriz de cultura y apropiación con los temas relacionados a seguridad de la información

Ejecución de la estrategia de cultura y apropiación en seguridad de la información	Líder de Seguridad	Febrero 2026	Diciembre 2026	Llevar a cabo las acciones que fomenten la cultura organizacional en materia de seguridad de la información
Medición de apropiación en seguridad de la información	Líder de Seguridad	Enero 2026	Diciembre 2026	Ejecutar acción programada que permita medir la apropiación de los conceptos/procedimientos de seguridad en la Entidad.

OPERACIÓN - IMPLEMENTACIÓN

La dependencia encargada de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es el GIT Tecnologías de la información y las comunicaciones.

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
MSPI	Líder de Seguridad	Febrero 2026	Abril 2026	Actualizar autodiagnóstico del MSPI
Controles NTC/IEC ISO 27001:2022	Líder de Seguridad	Febrero 2026	Diciembre 2026	Definir y actualizar de controles de seguridad de la información. Matriz de Declaración de Aplicabilidad
Gestión de Vulnerabilidades	Líder de Seguridad / GIT TICS	Marzo 2026	Diciembre 2026	Elaborar el plan de análisis de vulnerabilidades, alcance y coordinar ejecución pruebas

OPERACIÓN GESTIÓN DE INCIDENTES

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Sensibilización sobre incidentes de seguridad.	Líder de Seguridad	Enero 2026	Diciembre 2026	Socializar la documentación creada/actualizada.
CSIRT PONAL / CSIRT / Comando Conjunto Cibernético - CCOC	Líder de Seguridad	Febrero 2026	Mensual	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad
Eventos / vulnerabilidades	Líder de Seguridad / GIT TICS	Enero 2026	Diciembre 2026	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI

OPERACIÓN - CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Prueba, mantenimiento y revisión de continuidad	Líder de Seguridad / Líder de Infraestructura	Semestral	Semestral	Ejecutar pruebas sobre las estrategias definidas e implementadas Alinear las estrategias de seguridad con Plan de continuidad de negocio (BCP), Plan de recuperación ante desastres (DRP)

EVALUACIÓN DE DESEMPEÑO

La gestión de indicadores permite evaluar la eficacia, eficiencia y efectividad de las políticas y controles de seguridad de la información implementados en el Ministerio del Deporte

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Indicadores MSPI	Líder de Seguridad / Equipo GIT TICS	Enero 2026	Diciembre 2026	Revisar y actualizar de acuerdo con los objetivos del MSPI. Reportar seguimiento de los indicadores

MEJORAMIENTO CONTINUO

Actividad	Responsable	Fecha Inicio	Fecha Finalización	Descripción
Mejora	Líder de Seguridad / Equipo GIT TICS	Junio 2026	Diciembre 2026	Planes de acción para la remediación de no conformidades. Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar. Participar en las mesas intersectoriales y acoger las recomendaciones que se Emitan.

6. MARCO JURÍDICO

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".

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”.

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”.

ISO 27001:2022 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información.

ISO 22301:2012 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de continuidad del negocio

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