



**Deporte**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**  
**VIGENCIA**

**MINISTERIO DEL DEPORTE**

**GRUPO INTERNO DE TRABAJO TIC**

**BOGOTÁ D.C. ENERO DE 2024**

**VERSIÓN 3**

## TABLA DE CONTENIDO

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| 1. INTRODUCCIÓN .....                                                 | 3  |
| 2. OBJETIVO .....                                                     | 3  |
| 3. ALCANCE.....                                                       | 3  |
| 4. RESULTADOS DE LA LÍNEA BASE DE SEGURIDAD DE LA INFORMACIÓN.....    | 4  |
| 5. DETALLE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ..... | 5  |
| 6. REFERENCIAS .....                                                  | 14 |

## **1. INTRODUCCIÓN**

De acuerdo con el Modelo Integrado de Planeación y Gestión (MIPG) y al decreto 1499 de 2017, dentro de las políticas de Gestión y Desempeño Institucional se encuentran la planeación institucional, la gestión presupuestal y eficiencia del gasto público, el gobierno digital, la seguridad digital, entre otros ejes allí definidos. Asimismo, se establece que se debe asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, y que el sistema de gestión debe complementarse y articularse con los sistemas de gestión de seguridad de la información que se definan.

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. El resultado de esta fase en la Línea Base de Seguridad de la Información.

El presente documento desarrolla la fase de planificación, la cual consiste en la elaboración del plan de seguridad y privacidad de la información, alineado con el objetivo misional de la entidad y tiene como propósito definir las acciones a implementar a nivel de seguridad y privacidad de la información.

## **2. OBJETIVO**

Establecer y priorizar las actividades que están contempladas en el MSPI, las cuales están alineadas con el marco de referencia ISO 27001:2013 y la Política de Gobierno Digital.

## **3. ALCANCE**

El alcance del presente plan comprende la ejecución de acciones en la vigencia, tendientes a mejorar aspectos identificados en la línea base de seguridad de la información que establece la gestión de la entidad en 14 dominios de acuerdo a la ISO 27001:2013, dentro de la implementación del MSPI. Afecta a todos los procesos y activos de la información de la entidad y se desarrolla a través de tareas definidas con periodicidad mensual.

#### **4. RESULTADOS DE LA LÍNEA BASE DE SEGURIDAD DE LA INFORMACIÓN**

La línea base de seguridad de la información nos permite calificar el avance de la entidad de acuerdo con los dominios de la norma ISO 27001, asignando una calificación cuantitativa y cualitativa. La calificación cualitativa define los siguientes niveles:

- **Inexistente:** Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
- **Inicial:** Hay evidencia que la Organización ha reconocido que existe un problema y hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
- **Repetible:** Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
- **Efectivo:** Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
- **Gestionado:** Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
- **Optimizado:** Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

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

El Plan de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

| Dominio                                  | Actividades                                                                                     | ID  | Tareas                                                                                         | Responsable                                             | Inicio | Fin   |
|------------------------------------------|-------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------------|---------------------------------------------------------|--------|-------|
| POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad <i>Digital</i> | T01 | Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de                   | Líder de cada uno de los procesos                       | May -  | Jul - |
|                                          |                                                                                                 | T02 | Realimentación, revisión y verificación de los riesgos identificados                           | Encargado de seguridad de la información                | Jun -  | Jul - |
|                                          | Aceptación de Riesgos Identificados                                                             | T03 | Aprobación de Riesgos identificados y planes de tratamiento                                    | Comité institucional de coordinación de control interno | Jun -  | Jul - |
|                                          | Publicación de matrices de riesgos                                                              | T04 | Publicación de las matrices de riesgos en micrositios seguridad                                | Encargado de seguridad de la información                | Jul -  | Jul - |
|                                          | Seguimiento Fase de Tratamiento                                                                 | T05 | Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias | Enlaces del GIT planeación y Gestión de la OAP          | Nov -  | Dic - |
|                                          | Evaluación de riesgos residuales                                                                | T06 | Evaluación de riesgos residuales                                                               | Líder de cada uno de los procesos                       | Nov -  | Dic - |
|                                          | Mejoramiento de las matrices de riesgo                                                          | T07 | Identificación de oportunidades de mejora acorde a los resultados                              | Líder de cada uno de los procesos                       | Nov -  | Dic - |

|                                                |                                                             |     |                                                                                                                                                     |                                          |       |       |
|------------------------------------------------|-------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------|-------|
|                                                |                                                             |     | obtenidos durante la evaluación de riesgos residuales                                                                                               |                                          |       |       |
|                                                | Monitoreo y Revisión de riesgos                             | T08 | Generación, presentación y reporte de indicadores                                                                                                   | Líder de cada uno de los procesos        | Nov - | Dic - |
|                                                | Revisión Manual de Políticas de Seguridad de la Información | T09 | Actualizar la Políticas de Seguridad de la Información                                                                                              | Encargado de seguridad de la información | Mar - | May - |
|                                                | Protección de datos personales                              | T10 | Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos                                               | Encargado de seguridad de la información | May - | Jul - |
|                                                |                                                             | T11 | Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información | Encargado de seguridad de la información | Jul - | Jul - |
| ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | SGSI                                                        | T12 | Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información                           | Encargado de seguridad de la información | Oct - | Dic - |
|                                                |                                                             | T13 | Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente                                           | Encargado de seguridad de la información | Nov - | Dic - |

|                                   |                                                                                                                                          |     |                                                                                                                                                                                                                                                               |                                          |       |       |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------|-------|
|                                   |                                                                                                                                          | T14 | Revisar el avance de implementación del Plan de Seguridad y Privacidad en la Entidad                                                                                                                                                                          | Encargado de seguridad de la información | Nov - | Dic - |
|                                   |                                                                                                                                          | T15 | Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información                                                                                           | Encargado de seguridad de la información | Nov - | Dic - |
|                                   | Provisión de información a los indicadores de medición del SGSI                                                                          | T16 | Formular, Implementar y actualizar los indicadores del SGSI                                                                                                                                                                                                   | Encargado de seguridad de la información | Nov - | Dic - |
|                                   |                                                                                                                                          | T17 | Reportar indicadores                                                                                                                                                                                                                                          | Encargado de seguridad de la información | Nov - | Dic - |
| SEGURIDAD DE LOS RECURSOS HUMANOS | Fortalecer en el personal y contratistas, la comprensión de sus responsabilidades e idoneidad en los roles para los que son considerados | T18 | Seguir y actualizar los acuerdos contractuales con empleados y contratistas, se establecen sus responsabilidades y las de la organización en cuanto a la seguridad de la información (Cláusula 15 de contratación y Circular 11 de de la Secretaría General). | Oficina de Contratación                  | Nov - | Dic - |

|                       |                                                                                                                                                    |     |                                                                                                                         |                                                                      |       |       |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------|-------|
|                       | Elaborar el Plan de Gestión de Cultura Organizacional de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación | T19 | Actualizar el documento del Plan de Gestión de Cultura Organizacional                                                   | Encargado de seguridad de la información                             | Mar - | May - |
|                       |                                                                                                                                                    | T20 | Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos | Encargado de seguridad de la información                             | May - | May - |
|                       | Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación                  | T21 | Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI                       | Oficina de comunicaciones / Encargado de seguridad de la información | May - | Dic - |
|                       | Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación                  | T22 | Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI             | Encargado de seguridad de la información                             | May - | Dic - |
| GESTIÓN DE<br>ACTIVOS | Definir lineamientos para el levantamiento de activos de información                                                                               | T23 | Actualización de metodología e instrumento de levantamiento de activos de información                                   | Encargado de seguridad de la información                             | Mar - | May - |
|                       | Levantamiento de Activos de Información                                                                                                            | T24 | Socializar la guía de activos de Información                                                                            | Encargado de seguridad de la información                             | May - | May - |
|                       |                                                                                                                                                    | T25 | Validar activos de información en el instrumento levantado en la vigencia anterior                                      | Encargado de seguridad de la información                             | May - | May - |

|                   |                                                                                   |     |                                                                                                                                                                                                                                                                                                                                                                                                                        |                                          |       |       |
|-------------------|-----------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------|-------|
|                   |                                                                                   | T26 | Identificar nuevos activos de información en cada dependencia                                                                                                                                                                                                                                                                                                                                                          | Líder de cada uno de los procesos        | May - | Jun - |
|                   |                                                                                   | T27 | Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones                                                                                                                                                                                                                                                                                                                    | Encargado de seguridad de la información | May - | Jun - |
|                   |                                                                                   | T28 | Realizar correcciones a los instrumentos de activos de Información                                                                                                                                                                                                                                                                                                                                                     | Líder de cada uno de los procesos        | May - | Jun - |
|                   |                                                                                   | T29 | Informar sobre actualizaciones a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, materialización de riesgos que cambien la criticidad del activo | Líder de cada uno de los procesos        | Nov - | Dic - |
|                   | Publicación de Activos de Información                                             | T30 | Consolidar el inventario de activos de Información                                                                                                                                                                                                                                                                                                                                                                     | Encargado de seguridad de la información | May - | Jun - |
|                   |                                                                                   | T31 | Publicar el inventario de activos de información consolidada en el portal de la entidad                                                                                                                                                                                                                                                                                                                                | Administrador del portal web             | Nov - | Dic - |
|                   | Reporte Datos Personales                                                          | T32 | Reportar la información recolectada en el inventario de activos de información, correspondiente a bases de datos                                                                                                                                                                                                                                                                                                       | Encargado de seguridad de la información | Jun - | Jul - |
| CONTROL DE ACCESO | Limitar el acceso a información y a instalaciones de procesamiento de información | T33 | Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información                                                                                                                                                                                                                                                                             | Encargado de seguridad de la información | Abr - | Jul - |

|                                |                                                                                                                                |     |                                                                                                                                                                                                                      |                                        |       |       |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------|-------|
|                                |                                                                                                                                |     | que hayan sido autorizados específicamente.                                                                                                                                                                          |                                        |       |       |
| SEGURIDAD FÍSICA Y DEL ENTORNO | Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de | T34 | Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado                                                                  | Responsable de seguridad física        | Nov - | Dic - |
|                                | Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización               | T35 | Propender porque los equipos estén ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado;                                                 | Responsable de soporte y mantenimiento | Nov - | Dic - |
|                                |                                                                                                                                | T36 | Propender porque los equipos se protejan contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro; teniendo en cuenta los                                                  | Responsable de soporte y mantenimiento | Nov - | Dic - |
|                                |                                                                                                                                | T37 | Propender porque los equipos se protejan contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro; teniendo en cuenta los recursos dispuestos por la entidad para tal fin. | Responsable de soporte y mantenimiento | Mar - | Dic - |
|                                |                                                                                                                                | T38 | Realizar los mantenimientos preventivos y correctivos a todos los equipos de la entidad de acuerdo con el cronograma establecido.                                                                                    | Responsable de soporte y mantenimiento | Jul - | Dic - |

|                              |                                |     |                                                                                                                                        |                                                          |       |       |
|------------------------------|--------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-------|-------|
| SEGURIDAD DE LAS OPERACIONES | Vulnerabilidades               | T39 | Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades                                               | Encargado de seguridad de la información                 | Mar - | Jun - |
|                              |                                | T40 | Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida                              | Encargado de seguridad de la información                 | Jul - | Oct - |
|                              |                                | T41 | Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest | Responsable de cada uno de los sistemas según asignación | Oct - | Dic - |
|                              | Auditorías Internas y Externas | T42 | Participar en las auditorías internas y externas programadas, de acuerdo a la norma ISO 27001:2013                                     | Encargado de seguridad de la información                 | Nov - | Dic - |

|                                                     |                                                                                                                                 |     |                                                                                                                                                                                          |                                          |       |       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------|-------|
| SEGURIDAD DE LAS COMUNICACIONES                     | Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte           | T43 | Actualizar las directrices para la gestión de seguridad de redes                                                                                                                         | Encargado de seguridad de la información | Jul - | Oct - |
|                                                     |                                                                                                                                 | T44 | Actualizar las directrices para la gestión de la seguridad de los servicios de red                                                                                                       | Encargado de seguridad de la información | Jul - | Oct - |
|                                                     | Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.                 | T45 | Mapear los flujos de comunicaciones y datos                                                                                                                                              | Encargado de arquitectura empresarial    | Mar - | Jun - |
|                                                     |                                                                                                                                 | T46 | Actualizar las directrices para transferencia segura de información                                                                                                                      | Encargado de seguridad de la información | Mar - | May - |
|                                                     |                                                                                                                                 | T47 | Actualizar las directrices para mensajería electrónica                                                                                                                                   | Encargado de seguridad de la información | Mar - | May - |
|                                                     |                                                                                                                                 | T48 | Seguir y actualizar los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información (Cláusula 15 de contratación) | Oficina de Contratación                  | Nov - | Dic - |
| ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida | T49 | Definir las directrices para análisis y especificaciones de requisitos de seguridad de la información en sistemas nuevos o mejoras a los existentes                                      | Encargado de seguridad de la información | Mar - | Jun - |
|                                                     |                                                                                                                                 | T50 | Definir las directrices para los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y                         | Encargado de seguridad de la información | Mar - | Jun - |

|                                                      |                                                                   |     |                                                                                                                                      |                                          |       |       |
|------------------------------------------------------|-------------------------------------------------------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------|-------|
|                                                      |                                                                   |     | divulgación y modificación autorizadas no                                                                                            |                                          |       |       |
| RELACIONES CON LOS PROVEEDORES                       | Seguridad de la información en las relaciones con los proveedores | T51 | Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores | Encargado del contrato con proveedores   | Nov - | Dic - |
| GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | Gestionar los incidentes de                                       | T52 | Gestionar los incidentes de seguridad de la Información                                                                              | Encargado de seguridad de la información | Nov - | Dic - |
|                                                      | Eventos/vulnerabilidades                                          | T53 | Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI                                                   | Encargado de seguridad de la información | Nov - | Dic - |

## 6. REFERENCIAS

ISO 27001:2013 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

LEY 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1008 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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015

Manual para la implementación de la Política de Gobierno Digital

ELABORÓ: GIT TIC's