ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACION Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTI-P-02

V.8

26/01/2026

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

La información en las entidades es, actualmente, uno de sus activos más importantes y valiosos. Su adecuada gestión es esencial para la toma de decisiones estratégicas, permitiendo que las organizaciones sean más competitivas, innovadoras y capaces de ofrecer bienes y servicios de calidad, junto con información confiable, ágil y precisa a sus clientes y usuarios.

Sin embargo, los activos de información están cada vez más expuestos a ataques constantes, lo que ha llevado a un aumento significativo en los incidentes de seguridad de la información a nivel global. Estas brechas generan consecuencias graves para las empresas, como la pérdida de reputación, conflictos con clientes, pérdidas económicas y problemas legales.

Es por la importancia de la información, que el Instituto Distrital de las Artes – IDARTES, a través del presente documento establece la planificación, implementación, evaluación y mejora del Modelo de Seguridad y Privacidad de la Información-MSPI, determinado por las necesidades, objetivos, estructura organizacional, los procesos de la Entidad, así como requisitos legales y exigencias de seguridad de la información dadas por el Ministerio de las TIC establecido en el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3 Principios, que define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 que define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; así como la Resolución 00500 de 2021, la Resolución 02277 de 2025 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

En atención a esto el IDARTES tiene como propósito de avanzar en su transformación digital incluyó en su Plan Estratégico Institucional de 2026 los lineamientos de la Política de Gobierno Digital y Seguridad Digital a través de diversas iniciativas estratégicas de fortalecimiento institucional, participación y empoderamiento de ciudadano, arquitectura empresarial y seguridad de la información.

2. OBJETIVOS

2.1 Objetivo General

Diseñar, implementar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI) alineado con la norma NTC/IEC ISO 27001:2022, la matriz de aplicabilidad (SoA), la Política Digital, Seguridad y Privacidad de la Información, el Plan de Continuidad de Tecnologías de la Información y demás documentos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI) del IDARTES. Con el fin de garantizar la protección y preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.

2.2 Objetivos Específicos

- Implementar y realizar el seguimiento a los controles ISO27001:2022 a través de la Política Digital, Seguridad y Privacidad de la Información y el MSPI.
- Gestionar y tratar los riesgos de seguridad de la información de una manera sistemática, documentada y eficiente.
- Implementar los controles, lineamientos, normativas y directrices nacionales y distritales de obligatorio cumplimiento para las entidades públicas.
- Evaluar la eficacia y eficiencia de los controles implementados a través de la Matriz de Aplicabilidad SoA.
- Gestionar los incidentes de seguridad de la información que generen afectación sobre la operación de la entidad.
- Implementar estrategias de uso y apropiación de seguridad y privacidad de la información al interior del IDARTES.

3. ALCANCE

Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con las normas ISO 27001 e ISO 27032, así mismo, con los lineamientos incorporados con la Resolución 00500 de 2021 para el fortalecimiento de la gestión de la Política de Seguridad Digital y Continuidad de la operación para implementar dentro del Instituto Distrital de las Artes – IDARTES.

4. RESPONSABLES

Oficina Asesora de Planeación y Tecnologías de la Información (OAPTI).

5. DEFINICIONES

- **Activos de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.
- **Amenaza:** Según ISO/IEC 13335-1:20041 causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- **Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Integridad:** Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Política de Seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.
- **Seguridad de la Información:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. CONDICIONES GENERALES

Parte fundamental del Plan, para el diseño y planificación del Modelo de Seguridad y Privacidad de la Información (MSPI) el cual debe ser conocido por todo el IDARTES, así como tener en cuenta los compromisos y normatividad establecida por el Ministerio de las Tecnologías de la Información y Comunicaciones (MINTIC) y la Alta Consejería Distrital de TIC (ACDTIC) para las entidades gubernamentales; como lineamientos, políticas y directrices establecidas, según la De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

Por otra parte, el resumen ejecutivo Técnico y Administrativo del Instituto, los instrumentos y guías diseñados por el MINTIC, se tomaron como base para establecer la implementación del Modelo de Seguridad de la Información - MSPI, mediante la formulación de iniciativas, estrategias que garanticen el apoyo y cumplimiento de sus objetivos y funciones, que soporte adecuadamente los procesos misionales, estratégicos, transversales, de evaluación y mejora; entendiendo que a través de la Oficina Asesora de Planeación y Tecnologías de la Información es quien liderar la política de MIPG Seguridad Digital y Gobierno Digital alineado con el Plan estratégico institucional. Es importante mencionar en esta instancia, que la Oficina Asesora de Planeación y Tecnologías de la Información tiene como función formular y liderar el diseño, planeación, implementación y control de las actividades y productos asociados a la seguridad y privacidad de la Información, garantizando la integridad y debida custodia de

la información, en línea con la normatividad y legislación vigente y la Política de Gobierno Digital, abordando los siguientes aspectos:

- Formulación, actualización y divulgación de temas específicos referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.
- Continuar con la implementación del Modelo de Seguridad y Privacidad de la Información del IDARTES.
- Salvaguardar la información producida y procesada por las unidades de gestión del IDARTES.
- Administrar, controlar y gestionar los incidentes de la seguridad de la información.
- Optimización de sistemas de apoyo a la infraestructura tecnológica del IDARTES.

7. DESARROLLO DEL PLAN

7.1 Autodiagnóstico

El IDARTES, por ser una Entidad del orden Distrital que debe dar cumplimiento a las metas establecidas por MINTIC, en Seguridad de la Información, elemento habilitador de la Política de Gobierno Digital, para la estructuración del contexto, análisis, e implementación se utilizaron herramientas de diagnóstico definidas por los entes rectores en lineamientos para dar complimiento a la estrategia de apropiación de las Políticas de Gobierno Digital y Seguridad Digital.

Conforme a lo enunciado a continuación se plasman los resultados obtenidos de la valoración con el Instrumento Evaluación MSPI realizado en el cuarto trimestre de 2025 con el fin de reflejar el panorama actual de la entidad en el marco de la apropiación del gobierno digital en lo referente a la seguridad y privacidad de la información.

8. SITUACIÓN ACTUAL

El IDARTES es una entidad pública del orden distrital, con personería jurídica, autonomía administrativa, financiera y patrimonio propio, encargado de garantizar el ejercicio de los derechos culturales, mediante la promoción de las artes en el Distrito Capital, contribuyendo al desarrollo de sujetos creativos, sensibles, respetuosos de la diferencia, aportando a la construcción de una ciudad incluyente y solidaria.

La mayoría de la información generada en las diferentes Unidades de Gestión requiere de controles efectivos, de procedimientos internos para que permita brindar las condiciones para custodiar sus datos, sistemas de información, plan de tratamientos de riesgos de seguridad y privacidad de la información y acción para el uso y salvaguarda de la información. Por lo anterior, es pertinente y necesario planear y continuar con la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información - MSPI en el IDARTES de manera gradual y transversal, en sus procesos. El Modelo de Seguridad y Privacidad de la Información permitirá aplicar los controles pertinentes que garanticen la protección de los activos de información, que minimicen y prevengan inconvenientes legales, pérdidas económicas y daño reputacional, así como garantizar el cumplimiento de planes, programas, proyectos, metas y objetivos. Adicionalmente, permitirá al IDARTES cumplir con las exigencias normativas y legales establecidas por MinTIC en el elemento habilitador de Seguridad

Digital, según la Resolución 00500 de 2021 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

9. JUSTIFICACIÓN

La Oficina Asesora de Planeación y Tecnologías de la Información, luego de revisar el seguimiento de valoración del autodiagnóstico 2025, el cual arrojó como resultado un avance frente al compromiso del plan de acción integral con los lineamientos de ACDTIC y de MinTIC de cumplir al 70%; ha evidenciado un avance significativo y mejora continua frente a la implementación de los controles ISO 27001:2022 en los diferentes activos de información de la entidad.

Es responsabilidad del IDARTES continuar con la implementación de acciones que permitan el tratamiento de los riesgos de seguridad y privacidad de la información, así como el recurso humano suficiente para lograr el cumplimiento de los objetivos misionales y administrativos del instituto, por lo tanto, es necesario establecer los controles necesarios para identificar las causas y consecuencias de la materialización de los riesgos. Por lo cual, este plan pretende trazar la ruta a seguir para orientar y facilitar la gestión de la seguridad y privacidad de la información, de forma eficiente y efectiva, desde la identificación hasta la definición de controles para su gestión.

Ilustración 1. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

10. EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

Conforme a los lineamientos de la ISO 27001:2022 ANEXO A, a continuación, se presentan los resultados del Instrumento de Identificación de la Línea Base de Seguridad a corte de diciembre de 2025.

11. AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

La siguiente ilustración representa el avance de funcionamiento del modelo implementado

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación	Calificación	Nivel de
A.5	CONTROLES ORGANIZACIONALES	73	100	GESTIONADO
A.6	CONTROLES DE PERSONAS	58	100	EFECTIVO
A.7	CONTROLES FÍSICOS	93	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	57	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		70	100	GESTIONADO

Ilustración 2. Resultados evaluación controles ISO 27001-2024 (Fuente: instrumento MSPI - MINTIC)

12. ANÁLISIS DE RESULTADOS

En el documento se puede apreciar la calificación obtenida en cada uno de los controles y la calificación objetivo versus la meta establecida, que debió cumplir el Instituto el 31 de diciembre de 2025.

Ahora bien, frente al avance del Instituto al último trimestre de 2025, la Oficina Asesora de Planeación y Tecnologías de la Información realizó nuevamente el autodiagnóstico el cual dio como resultado un porcentaje de efectividad de los controles ISO 27001:2022 Anexo A del 70%.

Tabla de Escala de Valoración de Controles ISO 27001:2022 ANEXO A		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.

Tabla de Escala de Valoración de Controles ISO 27001:2022 ANEXO A		
Descripción	Calificación	Criterio
Repetible	40	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	60	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	80	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	100	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.

Ilustración 3. Nivel de madurez modelo seguridad y privacidad de la información (Fuente: https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacionMSPI)

Implementar controles

El IDARTES en la vigencia 2025 actualizó la Política Digital, Seguridad y Privacidad de la Información a los instrumentos de gestión de tecnología, articulado con el Modelo Integrado de gestión y Planeación – MIPG, incorporando los lineamientos de la Resolución 0500 de 2021 y el Modelo de Seguridad y Privacidad de la Información.

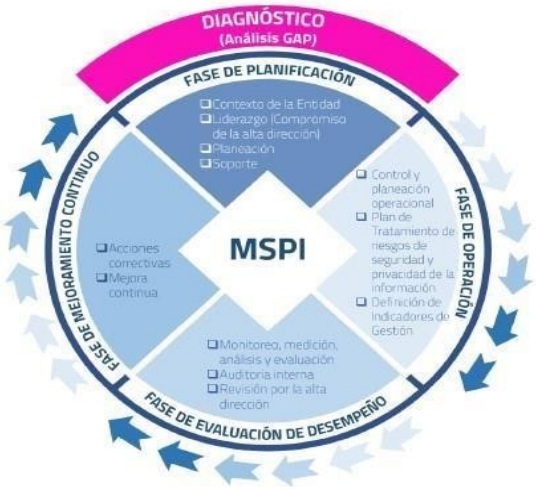

Ilustración 4. Ciclo del Modelo de Seguridad y Privacidad de la Información (Fuente: https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno- Digital/150507:Instrumento-de-evaluacion-MSPI)

Por lo anterior, el elemento habilitador de Seguridad de la Información se alinea con el modelo PHVA, y se engrana a través de cinco (5) fases, las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información, por lo tanto, desde la OAPTI se abordan las siguientes fases:

- **Diagnóstico**: Actualizar el diagnóstico, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI.
- **Planificación**: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta el contexto de interno y externo del IDARTES.
- **Operación**: Continuar con la implementación de los controles permiten disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
- **Evaluación de desempeño**: Determinar el sistema y forma de evaluación de la adopción del modelo, a través del seguimiento del indicador establecido para el MSPI.
- **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

En la fase de implementación del MPSI, según las necesidades y requerimientos del IDARTES con actividades correspondientes a la documentación de políticas, procedimientos, manuales, guías y demás mecanismos solicitados en los controles se dividen en dos sub- fases ya que para realizar las actividades de la fase de planeación se requiere actualizar el inventario de activos de información y otras actividades iniciales pertenecientes al proceso de Gestión TIC.

Conforme a la Política Digital, Seguridad y Privacidad de la Información el Autodiagnóstico de evaluación del MSPI 2024, se plantean acciones para abordar la implementación en el 2025 del Plan de Seguridad y Privacidad de la Información, el Modelo de Seguridad y Privacidad de la Información-MSPI, la Política de Seguridad Digital y la del IDARTES.

13. CRONOGRAMA IMPLEMENTACIÓN DEL PLAN

A continuación, se detallan las actividades previstas para la implementación del Plan de Seguridad y Privacidad de la Información durante el año 2026:

Ilustración 5. Cronograma de actividades

14. CONTROL Y SEGUIMIENTO

1. Autocontrol por parte de la primera línea de defensa (TI), mediante el uso del instrumento de gestión interno PETI.
2. Autoevaluación o monitoreo por parte de la segunda línea de defensa (OAP-TI), utilizando el instrumento de plan de acción integral 2025.
3. Evaluación independiente por parte de la tercera línea de defensa, a cargo del área de Control Interno.

Es importante conocer de manera permanente los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital y Seguridad Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de éstos en el Comité de Gestión Institucional y Desempeño, como lo establece el MIPG. La Oficina Asesora de Planeación y Tecnologías de la Información debe realizar el seguimiento y control a la implementación y/o mantenimiento de la Seguridad de la Información.

Ajustes y modificaciones:

Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el plan de seguridad y privacidad de la información, en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo:

En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con sus equipos realizarán el monitoreo permanente a la gestión de seguridad y privacidad de la información en coordinación con el oficial de seguridad de la información.

Seguimiento:

Coordinar en conjunto con la oficina de control interno, o quien haga sus veces, acciones para adelantar seguimiento a la gestión de seguridad y privacidad de la información, en este sentido, por esto, es necesario que en sus procesos de seguimiento interno analicen las causas, los riesgos y la efectividad de los controles incorporados en el documento.

15. NORMATIVIDAD

Para este plan, se aplica la normativa establecida en el nomograma institucional correspondiente al proceso de Gestión de Tecnologías de la Información.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2018-07-30	Emisión Inicial
2	2020-01-29	Proyección del plan según necesidades identificadas en la entidad
3	2021-01-14	Actualización normativa, autodiagnóstico y fases, riesgos, controles y actividades
4	2022-01-14	Actualización normativa, autodiagnóstico y fases, riesgos, controles y actividades
5	2023-01-31	Actualización Normativa, Autodiagnóstico y fases, riesgos, controles y actividades
6	2024-02-15	Actualización objetivos, definiciones, contenido y actividades a implementar en el 2024
7	2025-01-31	Se incorpora el cronograma de implementación del Plan de Seguridad y Privacidad de la Información, para el 2025.
8	2026-01-26	Actualización del cronograma de implementación del Plan de Seguridad y Privacidad de la Información, para el 2026.

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2026-01-21	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2026-01-21	MARIA CRISTINA HERRERA CALDERON	REFERENTE MIPG
APROBÓ	2026-01-26	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2026-01-26	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE
JONATHAN GONZALEZ BOLANOS