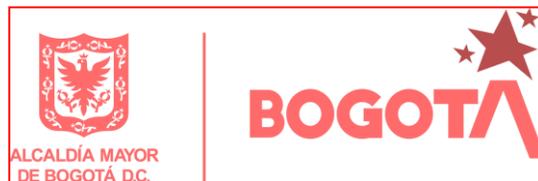




## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 2 de 27

<b>HISTÓRICO DE CAMBIOS</b>		
<b>Versión</b>	<b>Fecha de Emisión</b>	<b>Cambios realizados</b>
1	30 de julio de 2018	Emisión Inicial
2	29 de enero de 2020	Proyección del plan según necesidades identificadas en la entidad
3	14 de enero 2021	Actualización Normativa, Autodiagnóstico y fases, riesgos, controles y actividades
4	14 de enero 2022	Actualización Normativa, Autodiagnóstico y fases, riesgos, controles y actividades
5	31 de enero 2023	Actualización Normativa, Autodiagnóstico y fases, riesgos, controles y actividades
6	02 de febrero de 2024	Actualización objetivos, definiciones, contenido y actividades a implementar en el 2024.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 3 de 27

Elaboró	Revisó	Aprobó	Avaló
<p style="text-align: center;"><b>Maryury Forero Bohorquez</b> Contratista Oficina Asesora de Planeación y Tecnologías de la Información</p> <p style="text-align: center;"><b>Jorge Alberto Farigua Gutiérrez</b> Contratista Oficina Asesora de Planeación y Tecnologías de la Información</p>	<p style="text-align: center;"><b>Jonathan González</b> Profesional Universitario Oficina Asesora de Planeación y Tecnologías de la Información</p> <p style="text-align: center;"><b>María Cristina Herrera Calderón</b> Contratista Oficina Asesora de Planeación y Tecnologías de la Información</p>	<p style="text-align: center;"><b>Daniel Sánchez Rojas</b> Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información</p>	<p style="text-align: center;"><b>Daniel Sánchez Rojas</b> Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información</p>

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 4 de 27

## TABLA DE CONTENIDO

1. Introducción .....	7
2. Objetivos.....	8
2.1. Objetivo General.....	8
2.2. Objetivos específicos .....	8
3. Alcance .....	8
4. Responsables .....	9
5. Definiciones.....	9
6. Condiciones generales.....	10
7. Desarrollo documento .....	11
7.1. Diagnóstico y Autodiagnóstico.....	11
8. Situación actual .....	11
9. Justificación.....	12
10. Evaluación de efectividad de controles.....	13
11. Avance ciclo de funcionamiento del modelo de operación (PHVA) .....	13
12. Análisis de resultados .....	13
13. Implementar controles.....	16
14. Controles de Seguridad y Privacidad de la Información .....	17
15. Aplicabilidad SoA.....	19
16. Control y seguimiento .....	19
17. Normatividad.....	21

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 5 de 27

### Tabla de Ilustraciones

Ilustración 1. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032) .....13

Ilustración 2. Avance ciclo PVHA (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI>) .....13

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-evaluacion-MSPI>) .....14

Ilustración 4. Avance ciclo modelo operacional (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI>) .....14

Ilustración 5. Modelo Framework Ciberseguridad (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI>) .....15

Ilustración 6. 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>) .....16

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 6 de 27

### Tabla de Tablas

Tabla 1. Modelo Framework Ciberseguridad Nist.....	15
Tabla 2. controles de seguridad y privacidad de la información .....	17
Tabla 3. Normatividad.....	21

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 7 de 27

## 1. Introducción

La información en las empresas es considerada hoy en día uno de sus activos más importantes y valiosos, es de vital importancia para la toma de decisiones, para que las organizaciones sean más competitivas, innovadoras, presten mejores bienes, servicios y ofrezcan información confiable, ágil y acertada a sus clientes y usuarios. Sin dejar de mencionar que hoy por hoy los Activos De Información, son atacados constantemente, generando un aumento en el número de incidentes de seguridad de la información a nivel mundial que generan a las empresas pérdida de su buena imagen, problemas con sus clientes, pérdidas económicas y problemas legales, todo aunado a la presencia de la pandemia por Covid-19 que nos ha generado la necesidad imperativa de avanzar en la implementación y apropiación de nuevas tecnologías para el trabajo remoto, lo que impulsó la implementación de las estrategias TI enfocadas a la masificación del gobierno digital.

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, determinado por las necesidades, objetivos, estructura organizacional, los procesos misionales y tamaño de la Entidad, así como requisitos legales y exigencias de seguridad de la información dadas por MINTIC 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 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

La Política de Gobierno Digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura crítica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 8 de 27

En atención a esto el Idartes tiene como propósito de avanzar en su transformación digital incluyó en su Plan Estratégico Institucional 2020-2024 los lineamientos de la Política de Gobierno 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

Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información-MSPI, alineado con la NTC/IEC ISO 27001:2013, la matriz de aplicabilidad SoA, la Política de Seguridad y Privacidad de la Información y Continuidad de la Operación del Idartes, con el fin de proteger y preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

### 2.2. Objetivos específicos

- Formular e implementar controles a través de la Política de Seguridad y Privacidad de la Información.
- Gestionar y tratar los riesgos de seguridad de la información de una manera sistemática, documentada y eficiente.
- Aplicar los controles aplicables, lineamientos, normatividad y directrices nacionales y distritales de obligatorio cumplimiento para las entidades públicas.
- Planificar e implementar acciones que permitan mejorar los controles de seguridad y privacidad de la información.
- Evaluar la eficacia 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.
- Avanzar en la implementación de la estrategia de Seguridad Digital del Idartes.
- 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 fortaleciendo la gestión de la Política de

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 9 de 27

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

#### 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

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 10 de 27

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 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 Idartes 2020-2024. 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.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

- 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 documento

### 7.1. Diagnóstico y 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 cumplimiento 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 2023 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.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

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 2023, 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 49%; ha evidenciado que la mayoría de la información requiere mejoras de clasificación, controles administrativos, físicos y lógicos.

Es responsabilidad del Idartes implementar líneas de acción 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.

Razón por la cual es pertinente y necesario realizar la actualización e implementación del Modelo de Seguridad y Privacidad de la Información, no solo para dar cumplimiento a las metas establecidas por el MinTIC, si no para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información, así como crear una cultura organizacional que permita realizar y mantener un MSPI en el tiempo.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

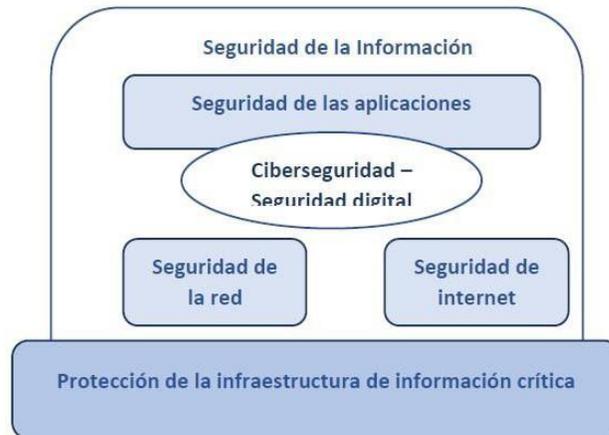


Ilustración 1. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

## 10. Evaluación de efectividad de controles

Conforme a los lineamientos de la ISO 27001:2013 ANEXO A, a continuación, se presentan los resultados del Instrumento de Identificación de la Línea Base de Seguridad a corte de diciembre de 2023.

## 11. Avance ciclo de funcionamiento del modelo de operación (PHVA)

La siguiente ilustración representa el avance de funcionamiento del modelo implementado

Año	AVANCE PHVA			
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado	
2023	Planificación	25%	40%	
	Implementación	13%	20%	
	Evaluación de desempeño	7%	20%	
	Mejora continua	4%	20%	
<b>TOTAL</b>		<b>49%</b>	<b>100%</b>	

Ilustración 2. Avance ciclo PHVA (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI>)

## 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 2023.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código: GTI-P-02</b>
		<b>Fecha: 02-02-2024</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 06</b>
		<b>Página: 11 de 27</b>

Ahora bien, frente al avance del Instituto al último trimestre de 2023, 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 27001:2013 Anexo A del 49% y de un 49% en el ciclo PHVA, aumentando 11 puntos porcentuales comparado con la anterior vigencia.

		NIVEL DE CUMPLIMIENTO	Nivel	Descripción
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	SUFICIENTE	Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.
	Repetible	SUFICIENTE	Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente planificación del MSPi.
	Definido	INTERMEDIO	Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
	Administrado	CRÍTICO	Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorías al MSPi, recolectando información para establecer la efectividad de los controles.
	Optimizado	CRÍTICO	Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPi, retroalimentando cualitativamente el modelo.

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-evaluacion-MSPI>)

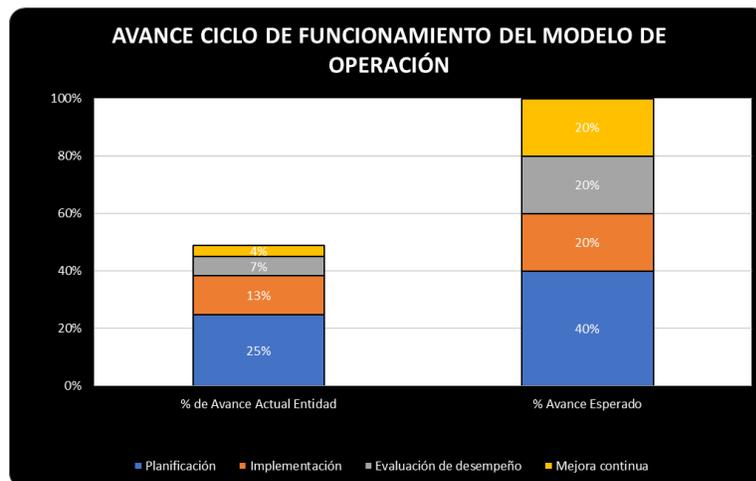


Ilustración 4. Avance ciclo modelo operacional (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI>)

Como se evidencia en el grafico siguiente, a nivel de ciberseguridad se avanzó en la ejecución de controles en el marco de los lineamientos de la resolución 00500 de 2021, abordando las actividades del plan de tratamiento de riesgos de la seguridad de la información 2023 y el plan de seguridad y privacidad de la información 2023 los cuales al cuarto trimestre obtuvieron los siguientes resultados

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Fecha:</b> 02-02-2024
		<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Tabla 1. Modelo Framework Ciberseguridad Nist

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCIÓN CSF	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
DETECTAR	53,8	100
IDENTIFICAR	46,0	100
PROTEGER	46,9	100
RECUPERAR	53,3	100
RESPONDER	53,3	100

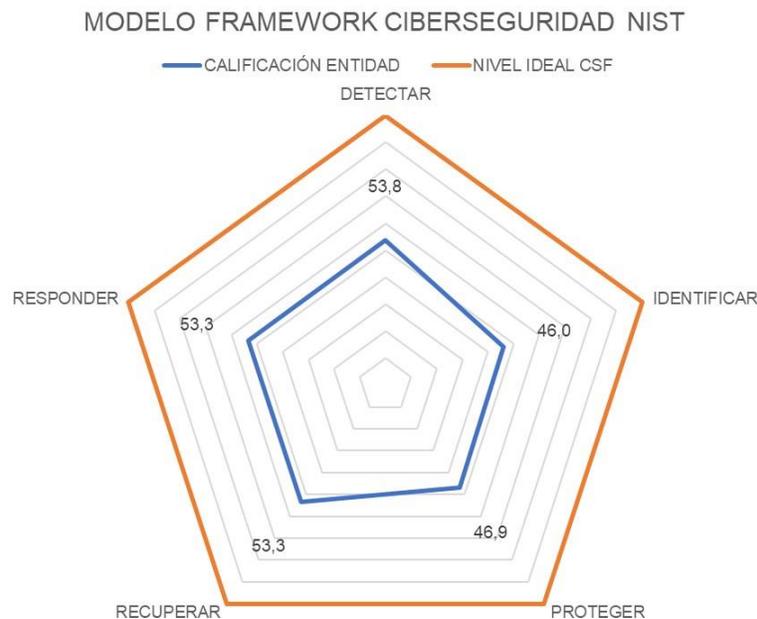


Ilustración 5. Modelo Framework Ciberseguridad (Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI> )

Así mismo, con la actualización de la herramienta de autodiagnóstico se presentan avances en seguridad de las operaciones y seguridad de las comunicaciones debido a cambios planteados en la gestión de antivirus en una consola centralizada en la nube permitiendo controlar los equipos instalados en las sedes del Idartes y los CREA, además de los ajustes en la configuración del firewall permite optimizar el uso del canal y administrar el consumo por usuario.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

### 13. Implementar controles

El Idartes en la vigencia 2023 actualizó la Política de 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.

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:

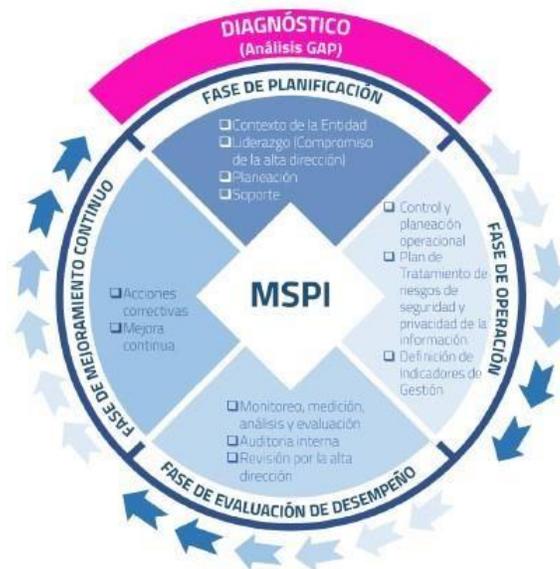


Ilustración 6. Ciclo del Modelo de Seguridad y Privacidad de la Información  
(Fuente: <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150507:Instrumento-de-evaluacion-MSPI> )

- **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.

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> <small>CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</small>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

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 de Seguridad y Privacidad de la Información y el Autodiagnóstico de evaluación del MSPI 2023, se plantean los siguientes controles para abordar la implementación en el 2024 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 Política de Seguridad y Privacidad de la Información del Idartes.

#### 14. Controles de Seguridad y Privacidad de la Información

A continuación, se presentan los controles (administrativos y técnicos) de seguridad y privacidad de la información

*Tabla 2. controles de seguridad y privacidad de la información*

<b>Control</b>	<b>Actividades</b>	<b>Responsable</b>	<b>Fecha máxima</b>
Políticas de seguridad de la información	Socializar las políticas de seguridad y privacidad de la información	OAP-TI	31/12/2024
Responsabilidades y organización seguridad información	Implementar estrategias de uso y apropiación relacionadas con aspectos de seguridad y privacidad de la información a toda la comunidad del Idartes.	OAP-TI	31/12/2024
Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	Actualizar el inventario de activos de información con la clasificación de seguridad y privacidad de la información.	OAP-TI	31/07/2024
Asegurar que la información recibe un	Realizar revisión de la matriz de riesgos de seguridad de la	OAP-TI	31/12/2024

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Control	Actividades	Responsable	Fecha máxima
nivel apropiado de protección, de acuerdo con su importancia para la Entidad.	información y actualizar en caso de ser necesario teniendo en cuenta los cambios del entorno de la entidad y la normatividad vigente		
Control de acceso a códigos fuente de programas	Restringir el acceso a los códigos fuente de los programas.	OAP-TI	31/12/2024
Equipos de usuario desatendidos	Asegurar los equipos desatendidos de los usuarios con políticas de protección.	OAP-TI	31/12/2024
Registros del administrador y del operador	Registrar las actividades del administrador y del operador del sistema.	OAP-TI	31/12/2024
Seguridad de los servicios de red	Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	OAP-TI	31/12/2024
Políticas y procedimientos de transferencia de información	Formular políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	OAP-TI	31/12/2024
Implementar una actividad de control de cambios para los	Elaborar y formalizar un formato para la gestión de cambios, con el cual se controlen los cambios que se efectúen en los sistemas	OAP-TI	31/12/2024

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Control	Actividades	Responsable	Fecha máxima
sistemas de información	de información, antes del paso a producción de los mismos.		
Mejora continua	Actualizar el procedimiento de Mantenimiento y Desarrollo de Software donde se incluyan actividades relacionadas con el Acuerdo 002 de 2023	OAP-TI	31/12/2024
Mejora continua	Formular y actualizar la documentación de los Planes de recuperación de desastres de TI y el plan de continuidad de negocio y realizar pruebas de acuerdo con la capacidad técnica instalada en el Idartes	OAP-TI	31/12/2024
Gestión de incidentes de seguridad	Revisar y actualizar procedimiento Incidentes de Seguridad de la Información en caso de ser necesario	OAP-TI	31/12/2024

## 15. Aplicabilidad SoA

La Declaración de Aplicabilidad, referenciado en el numeral 6.1.3d de la norma ISO-27001, a través del documento matriz de aplicabilidad SoA 27001 que lista los objetivos y controles que se van a implementar en la Entidad, en este entendido y conforme al análisis realizado para establecer los controles del presente plan, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO-27001, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar.

## 16. Control y seguimiento

En el marco de las líneas de defensa se debe realizar: Autocontrol por la primera línea de defensa (TI), Autoevaluación o monitoreo por la segunda línea de defensa (OAP-TI) y evaluación independiente por la tercera línea de defensa por el área de Control Interno

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

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.

Se debe revisar periódicamente por cada responsable de los procesos al interior de las unidades de gestión, y junto con el equipo los siguientes aspectos:

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.

Es importante realizar una socialización del plan vigente para que las unidades de gestión conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital y su eje transversal de seguridad. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos, para lo cual, los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Plan de Seguridad y Privacidad de la Información deben ser tratados a través de los gestores MIPG de ser necesario, para su óptimo cumplimiento, apoyados por el oficial de seguridad de la información.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

## 17. Normatividad

Tabla 3. Normatividad

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1360 de 1989	Presidencia de Colombia	Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
Decreto 2150 de 1995	Ministerio de Justicia y del Derecho	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Ley 572 de 1999	Congreso de la República	Comercio Electrónico, Firmas Digitales, Intercambio electrónico de datos.
Decreto 3816 de 2003	Presidencia de Colombia	Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública
Conpes 3292 de 2004	Departamento Nacional de Planeación	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
Directriz 5 de 2005	Alcaldía Mayor de Bogotá	Por la cual la Alcaldía Mayor de Bogotá define Políticas Generales y Directrices que orienten el desarrollo tecnológico.
Decreto 619 de 2007	Alcaldía Mayor de Bogotá	Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito.
Decreto 316 de 2008	Alcaldía Mayor de Bogotá	Por medio del cual se modifica parcialmente el artículo 3 del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Ley 1273 de 2009	Congreso de la República	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.

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

<b>Tipo de norma</b>	<b>Entidad que expide</b>	<b>Descripción normativa</b>
Ley 1341 de 2009	Congreso de la República	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 235 de 2010	Ministerio del Interior y de Justicia	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Conpes 3701 de 2011	Departamento Nacional de Planeación	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Ley 1581 de 2012	Congreso de la República	Por el cual se dictan disposiciones generales para la protección de datos personales
Decreto 884 de 2012	Presidencia de Colombia	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones
Decreto 2364 de 2012	Ministerio del Interior y Justicia	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones
Decreto 19 de 2012	Presidencia de Colombia	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
Resolución 396 de 2012	Instituto Distrital de las Artes	Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - Idartes.
Ley 1618 de 2013	Presidencia de Colombia	Por medio de la cual se establecen las disposiciones para garantizar el pleno ejercicio de los derechos de las personas con discapacidad. Art 16. Derecho a la información y comunicaciones
Decreto 1377 de 2013	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 596 de 2013	Alcaldía Mayor de Bogotá	Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital

	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Tipo de norma	Entidad que expide	Descripción normativa
ley 1712 de 2014	Congreso de la República	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
Resolución 383 de 2014	Instituto Distrital de las Artes	Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - Idartes".
Ley 1753 de 2015	Congreso de la República	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" 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 103 de 2015	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1081 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 1078 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Conpes 3854 de 2016	Departamento Nacional de Planeación	Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Decreto 415 de 2016	Departamento Administrativo de la Función Pública	Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Tipo de norma	Entidad que expide	Descripción normativa
Resolución 4 de 2017	Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	Por la cual se modifica la Resolución 305 de 2008 de la CDS
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico
Decreto 1413 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Resolución 2710 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se establecen lineamientos para la adopción del protocolo IPv6
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno
Circular 30 de 2017	Alta Consejería de TICs	Implementación CSIRT de Gobierno
Circular 36 de 2017	Alta Consejería de TICs	Lineamientos de avance del modelo de seguridad y privacidad de la información
Resolución 3436 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

<b>Tipo de norma</b>	<b>Entidad que expide</b>	<b>Descripción normativa</b>
Decreto 612 de 2018	Departamento Administrativo de la Función Pública	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 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	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
Circular 2 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Cumplimiento legal y normativo respecto a seguridad de la información
Conpes 3920 de 2018	Departamento Nacional de Planeación	Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Ley 1955 del 2019	Presidencia de Colombia	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Decreto 2106 de 2019	Departamento Administrativo De La Función Pública	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva
Conpes 3975 de 2019	Departamento Nacional de Planeación	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 620 de 2020	Departamento Administrativo De La Función Pública	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Resolución 00500 de 2021	Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC	“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 00500 de 2021 Anexo 1	Ministerio de las Tecnologías de la Información y las Comunicaciones	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las Entidades del Estado
Directiva 09 de 2021	Secretaría Jurídica Distrital	Buenas prácticas en el uso de fotografías y videos para la protección de derechos de autor
Resolución número 00460 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Se dictan disposiciones sobre el Plan Nacional de Infraestructura de datos
Decreto 338 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el título 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
Decreto 767 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	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

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes</p>	<b>GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN</b>	<b>Código:</b> GTI-P-02
		<b>Fecha:</b> 02-02-2024
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión:</b> 06
		<b>Página:</b> 11 de 27

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1263 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el título 22 a la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de definir lineamientos y estándares aplicables a la transformación digital pública
Decreto 1389 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el título 24 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 la gobernanza en la infraestructura de datos, y se crea el modelo de gobernanza de la infraestructura de datos
Decreto 1449 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adopta la estructura del Ministerio de Ciencia, Tecnología e Innovación y se dictan otras disposiciones; Art. 7 Num. 13
Acuerdo 002 de 2023	Alcaldía Mayor de Bogotá	Lineamiento para el desarrollo de evaluaciones de impacto a la privacidad



Radicado: 20244300079913

Fecha 02-02-2024 12:34

**Documento 20244300079913 firmado electrónicamente por:**

**JONATHAN GONZÁLEZ BOLAÑOS**, Profesional Universitario Código: 219 Grado: 01, Área de Tecnología, Fecha de Firma: 05-02-2024 12:09:25

**DANIEL SÁNCHEZ ROJAS**, Jefe Oficina Asesora de Planeación y Tecnologías de la Información, Oficina Asesora de Planeación, Fecha de Firma: 05-02-2024 19:39:53

**MARYURY FORERO BOHORQUEZ**, Contratista, Oficina Asesora de Planeación, Fecha de Firma: 02-02-2024 14:04:48

**JORGE ALBERTO FARIGUA GUTIERREZ**, , Oficina Asesora de Planeación, Fecha de Firma: 02-02-2024 15:32:59

**MARIA CRISTINA HERRERA CALDERON**, , Oficina Asesora de Planeación, Fecha de Firma: 02-02-2024 12:48:27

Proyectó: SANDRA PATRICIA MORENO BOHORQUEZ - Técnico Administrativo - Área de Tecnología



9107731d12403dcf64f84867efe9672ec8ad66259e2c298effd55a8d6ba15a35

En el marco de los lineamientos del numeral 6.5 de la "Guía diseño de documentos del sistema integrado de gestión – SIG", se actualiza el código del presente documento para que se articule con la codificación vigente relacionada en la señalada guía y en el Listado Maestro de Documentos. El contenido del documento no cambia.

