

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 1 de 14	

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	2
2.	OBJETIVO GENERAL.....	3
3.	ALCANCE	3
4.	NORMATIVIDAD.....	3
5.	DEFINICIONES.....	3
	RESPONSABLES Y ROLES	5
6.	PRINCIPIOS ORIENTADORES	8
7.	RUTA DE IMPLEMENTACIÓN.....	8
7.1.	COMPROMISO DE LA DIRECCIÓN	8
7.2.	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	9
7.3.	APLICABILIDAD.....	11
7.4.	SANCIONES	12
7.5.	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL MSPI	12
7.6.	REVISIÓN Y VIGENCIA.....	13
8.	BIBLIOGRAFIA	14
9.	CONTROL DE CAMBIOS	14
10.	AUTORIZACIONES	14

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 2 de 14	

1. INTRODUCCIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información – MSPI constituye un pilar fundamental para fortalecer la gestión institucional de los activos de información del Jardín Botánico José Celestino Mutis (JBJCM). Su propósito es desarrollar capacidades organizacionales que permitan incorporar, de manera sistemática y progresiva, los lineamientos de seguridad y privacidad en todos los procesos, trámites, servicios, sistemas de información, infraestructura tecnológica y, en general, en cualquier activo que almacene, procese o transmita información. Este modelo busca garantizar la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los datos, contribuyendo así al cumplimiento de los objetivos misionales y a la protección de los derechos de funcionarios, contratistas, proveedores y ciudadanía.

En concordancia con la normativa vigente aplicable a las entidades del Estado colombiano — incluyendo el Decreto 1078 de 2015, la Resolución 500 de 2021, su actualización mediante la Resolución 2277 de 2025, la política de seguridad digital del país y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG)— el Jardín Botánico establece los principios y lineamientos que orientan esta Política General de Seguridad y Privacidad de la Información. A través de la Oficina Asesora de Planeación, la Entidad liderará la planeación, implementación, capacitación, seguimiento y mejora continua de las acciones necesarias para gestionar los riesgos asociados a los activos de información, promoviendo su uso adecuado, seguro y responsable.

La Política General de Seguridad y Privacidad de la Información constituye la declaración formal mediante la cual el JBJCM expresa su postura institucional frente a la protección y gestión segura de sus activos de información, entendidos estos como: personas (funcionarios, contratistas y proveedores), información en todas sus formas, procesos organizacionales, infraestructura tecnológica, software, hardware y demás elementos que soportan la operación institucional. Esta política se convierte en el marco habilitador para la implementación del Subproceso de Seguridad de la Información (SDI) y para la definición de políticas específicas, procedimientos, lineamientos e instructivos que asignan roles y responsabilidades para la gestión adecuada de la seguridad y privacidad de la información.

El presente documento se estructura conforme a las mejores prácticas internacionales, incorporando los principios y requisitos establecidos en la ISO/IEC 27001, los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI, y las disposiciones de la Política de Seguridad Digital del MIPG. Su adopción permite al JBJCM avanzar hacia una gestión integral de la seguridad, asegurar la protección de los activos institucionales, fortalecer la confianza digital y garantizar el cumplimiento de la normativa aplicable.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 3 de 14	

2. OBJETIVO GENERAL

Establecer los lineamientos definidos por la Dirección del Jardín Botánico José Celestino Mutis (JBJCM) para la gestión de la seguridad y privacidad de la información, considerando la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), los lineamientos de Seguridad Digital y Gobierno Digital, los requisitos establecidos en la normativa vigente aplicable a las entidades públicas y las necesidades de las partes interesadas internas y externas.

2.1. OBJETIVOS ESPECÍFICOS

- Orientar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en todos los procesos, servicios, trámites, proyectos y sistemas del JBJCM.
- Fortalecer la cultura institucional de seguridad y privacidad de la información, promoviendo la sensibilización, la formación y la responsabilidad entre funcionarios, contratistas y terceros vinculados al JBJCM.
- Gestionar los riesgos de seguridad de la información con el fin de reducir la probabilidad e impacto de los incidentes, garantizando la continuidad operativa y la protección de los datos.

3. ALCANCE

La Política de Seguridad y Privacidad de la Información del Jardín Botánico de Bogotá José Celestino Mutis aplica a todos los niveles de la entidad y es de obligatorio cumplimiento para funcionarios, contratistas, proveedores, terceros y cualquier persona o entidad que acceda o gestione información del JBJCM, tanto de manera interna como externa. Cubre toda la información institucional, sin importar su formato, medio o ubicación, y abarca todos los procesos, sistemas, servicios y actividades, conforme al marco normativo vigente. Su implementación se fundamenta en los lineamientos de la Alta Dirección mediante la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), e incluye la identificación y clasificación de activos de información, la gestión de riesgos, la definición de controles y la aplicación de procedimientos y actividades operativas.

4. NORMATIVIDAD

La normatividad asociada al desarrollo de este documento se encuentra en el Normograma del Jardín Botánico José Celestino Mutis – JBJCM

5. DEFINICIONES

Las definiciones de la Política General de Seguridad y Privacidad de la Información del JBJCM, tiene fundamento en el estándar internacional ISO 27001¹.

A continuación, se listan algunas de las más importantes, relacionadas con la gestión de los documentos:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados (Ley 1712, 2014).

¹ <https://www.iso.org/standard/27001>

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 4 de 14	

- **Alcance del MSPI:** Es el número del total de los procesos que serán incluidos en la implementación del MSPI.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización (Modelo de Seguridad y Privacidad de la Información, 2025).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).
- **Análisis de riesgos:** Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo (Modelo de Seguridad y Privacidad de la Información, 2025).
- **Confidencialidad:** Propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. (ISO/CEI 27000, 2018).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados (Modelo de Seguridad y Privacidad de la Información, 2025).
- **Control:** Medida que modifica el riesgo. Sinónimo salvaguarda (ISO/CEI 27000, 2018).
- **Disponibilidad:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (ISO/CEI 27000, 2018).
- **Gestión de riesgos:** Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (ISO/CEI 27000, 2018).
- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022)
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712, 2014).
- **Integridad:** La propiedad de salvaguardar la exactitud y completitud de la información. (ISO/CEI 27000, 2018).
- **Modelo de Seguridad y Privacidad de la Información - MSPI:** lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un Sistema de Gestión de Seguridad y privacidad de la Información – SGSPI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando consideraciones y controles específicos de ciberseguridad en cada una de sus etapas (Modelo de Seguridad y Privacidad de la Información, 2025)
- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Modelo de Seguridad y Privacidad de la Información, 2025)
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).
- **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital(ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i)

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 5 de 14	

la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley Estatutaria 1581. Art 3, 2012).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/CEI 27000, 2018).

6. RESPONSABLES Y ROLES

El JBJCM a continuación define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados:

Tabla 1. Roles y responsabilidades de la política de seguridad y privacidad de la información

LINEA ESTRATEGICA	
RESPONSABLE	ROLES
Dirección del JBJCM	• Asignar, aprobar y proporcionar los recursos necesarios para la implementación y mantenimiento del MSPI (Recursos económicos, formación y recursos tecnológicos).
Comité Institucional de Gestión y Desempeño	• Cumplir con lo establecido en el Artículo III de la Resolución 289 de 2020 del JBJCM en cuanto a "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información"; así mismo, serán los encargados de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con el Modelo Integrado de Planeación y Gestión MIPG
PRIMERA LINEA DE DEFENSA	
RESPONSABLE	ROLES
Secretaria General – Proceso Gestión de la Tecnología	El Proceso de Gestión de Tecnología es responsable de administrar y controlar el acceso a los recursos de la plataforma tecnológica en el Jardín Botánico José Celestino Mutis de acuerdo con la descripción del cargo. Sus responsabilidades frente al SGSI son: • Definir e Implementar los controles a los activos tecnológicos que ayuden a mitigar los riesgos de seguridad de la información. • Apoyar en la mitigación de los procesos de gestión de vulnerabilidades para los activos de información asociados. • Apoyar en el levantamiento y reporte de activos de información y gestión de riesgos para los activos asociados al proceso. • Apoyar la ejecución de los incidentes de seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la Entidad, de acuerdo con sus competencias. • Monitorear a través de las herramientas tecnológicas de la Entidad el comportamiento del uso del servicio de Internet. • Verificar qué usuarios y/o contratistas tienen acceso remoto a los recursos de la Entidad • Asegurar el correcto funcionamiento y la disponibilidad que se requiere del servicio de Internet, sobre el cual se deben aplicar los controles que se definan

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 6 de 14	

	- Generar informes del uso del servicio, como medida preventiva de seguridad que permita tomar decisiones y realizar ajustes de configuración. - Gestionar los accesos a los servicios o sistemas de información que dependan del Jardín Botánico José Celestino Mutis, y solicitar aquellos que deban ser tramitados ante externos, de acuerdo con lo indicado por los responsables o dueños de los sistemas de información - Implementar y gestionar los controles de seguridad sobre los activos de información tecnológicos de la entidad. - Coordinar con el proceso de Seguridad de la Información el Plan de Sensibilización de Seguridad de la Información y Protección de Datos Personales en el JBJCM, para la toma de conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Secretaría General – Proceso Gestión Documental	- Implementar los controles a los activos tipo información física que ayuden a mitigar los riesgos de seguridad de la información - Participar en la identificación de riesgos relacionados con pérdida, alteración o destrucción de documentos - Identificar documentos que contienen información sensible, confidencial o pública, para consulta acorde al índice de información clasificada y reservada. - Velar por el cumplimiento de la Ley General de Archivos. - Actualizar los instrumentos archivísticos e índice de información.
Secretaría General – Proceso Gestión Contractual	- Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. - Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Secretaría General – Proceso Comunicaciones	Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles del JBJCM.
Secretaría General – Proceso Gestión del talento humano	Coordinar con el proceso de Seguridad de la Información el Plan de Sensibilización de Seguridad de la Información y Protección de Datos Personales en el JBJCM, para la toma de conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Todos los procesos	Implementar las políticas, procedimientos y controles de seguridad de la información que se definan como parte del MSPI (Por ejemplo: gestión de activos, gestión de riesgos, controles entre otros).
Funcionarios, contratistas y terceros	- Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. - Cumplir las políticas y procedimientos de seguridad de la información definidos y aprobados. - Informar sobre cualquier incidente de seguridad de la información por los canales establecidos - Asistir a las sensibilizaciones en temas de Seguridad de la Información. - Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera del JBJCM
SEGUNDA LINEA DE DEFENSA	
RESPONSABLE	ROLES
Oficina Asesora de Planeación – Proceso Seguridad de la Información	- Estructurar, orientar, liderar la implementación de la Política de Seguridad y Privacidad de la Información. - Analizar, definir, documentar y gestionar el Plan de Seguridad de la Información y proponer las acciones que permitan gestionar la seguridad de la información en

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 7 de 14	

	el marco del cumplimiento de la política y los lineamientos definidos y aprobados por la Entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos, manuales y guías) que permitan el establecimiento y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información MSPI. • Identificar y coordinar la reducción de la brecha entre el MSPI y la situación actual de la Entidad • Liderar y brindar acompañamiento a los procesos de la Entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas. • Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Prestar asistencia técnica en el análisis de resultados obtenidos y registrar los resultados de los análisis de vulnerabilidades y el reporte realizado en la base de conocimiento • Atender los incidentes de Seguridad de la Información y ejecutar actividades de seguimiento • Asesorar en materia de Seguridad de la Información a la entidad • Velar por el cumplimiento de la normativa de Protección de Datos Personales, incluyendo la Ley 1581 de 2012 y sus normas reglamentarias. • Coordinar las actividades relacionadas con el Tratamiento de Datos Personales dentro de la Entidad. • Realizar seguimiento periódicas de riesgos y vulnerabilidades en relación con el Tratamiento de Datos Personales, y tomar medidas para mitigar dichos riesgos. • Mantener actualizado el Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio - SIC incluyendo la información relacionada con las bases de datos administradas por la Entidad y los tratamientos de datos personales realizados, conforme a lo establecido en la normatividad vigente. • Asesorar a la organización en materia de protección de datos personales y ofrecer capacitación y orientación al personal sobre sus responsabilidades en relación con la protección de datos. • Coordinar la atención de consultas, solicitudes y reclamos relacionados con la protección de datos personales. • Actuar como enlace entre la organización y la SIC, en su calidad de autoridad de protección de datos personales, para atender requerimientos, facilitar auditorías y garantizar el cumplimiento de la normativa aplicable. • Verificar el cumplimiento de las políticas y procedimientos establecidos en la organización en relación con la protección de datos personales. • Colaborar con otras áreas de la entidad en la implementación de medidas de seguridad y privacidad de los datos personales.
TERCERA LINEA DE DEFENSA	
RESPONSABLE	ROLES
Oficina de Control Interno	• Incluir la seguridad de la información en los planes de auditoría institucionales. • Asesorar de forma coordinada con la Oficina Asesora de Planeación, a la primera línea de defensa respecto a las situaciones que puedan poner en riesgo el cumplimiento de la presente política.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 8 de 14	

	- Realizar actividades de seguimiento que faciliten la generación de alertas a la administración del proceso de seguridad de la información. - Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
--	---

Fuente: Elaboración propia

7. PRINCIPIOS ORIENTADORES

Los siguientes principios orientadores constituyen la base para la gestión adecuada de la seguridad y privacidad de la información en el JBJCM. Estos principios guían la toma de decisiones, el diseño de controles y la implementación de medidas para proteger los activos de información de la entidad.

- **Confidencialidad:** Garantizar que la información sea accesible únicamente a las personas, procesos o sistemas que cuenten con autorización expresa para ello. Este principio protege el carácter reservado de los datos, evitando su divulgación, exposición o acceso indebido.
- **Integridad:** Asegurar que la información se mantenga completa, precisa, consistente y libre de alteraciones no autorizadas durante su creación, almacenamiento, procesamiento, transmisión y consulta. La integridad preserva la confiabilidad y exactitud de los datos como fundamento para la toma de decisiones.
- **Disponibilidad:** Garantizar que la información y los servicios asociados estén accesibles y operativos cuando sean requeridos por los usuarios autorizados, de acuerdo con las necesidades del negocio y los niveles de servicio establecidos. La disponibilidad implica contar con mecanismos de continuidad, de recuperación y de gestión de incidentes que reduzcan las interrupciones y las afectaciones.

8. RUTA DE IMPLEMENTACIÓN

8.1. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección del Jardín Botánico de Bogotá José Celestino Mutis (JBJCM) declara su compromiso institucional con el establecimiento, la implementación, la operación, el mantenimiento y la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con el marco normativo vigente en materia de seguridad digital y gobierno de la información.

En cumplimiento de lo dispuesto en el Decreto 1078 de 2015, particularmente en lo referente a las responsabilidades del representante legal de los sujetos obligados para coordinar, hacer seguimiento y verificar la implementación de la Estrategia de Gobierno Digital, así como en la Resolución 500 de 2021 y su actualización mediante la Resolución 2277 de 2025, la Alta Dirección garantizará que la seguridad de la información, la gestión del riesgo digital y la privacidad sean consideradas como elementos estratégicos para el cumplimiento de la misión institucional y la prestación adecuada de los servicios del JBJCM.

Para ello, la Alta Dirección se compromete a:

- Liderar, promover y respaldar el establecimiento, la implementación y la mejora continua del SGSI y del MSPI, asegurando su alineación con la estrategia institucional y con los requisitos normativos aplicables.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 9 de 14	

- Asignar y gestionar los recursos necesarios, incluyendo infraestructura tecnológica, herramientas, procesos y talento humano competente, que permitan la implementación, operación y sostenibilidad correctas del modelo.
- Revisar periódicamente, al menos semestralmente, el desempeño, el nivel de avance y los resultados del SGSI/MSPI, adoptando decisiones orientadas al cierre de brechas y a la mejora continua.
- Integrar la seguridad y la privacidad de la información en los procesos de planeación, toma de decisiones y gestión estratégica, como parte fundamental de la gobernanza organizacional.

Con este compromiso, la Alta Dirección asegura el liderazgo institucional y el respaldo requerido para fortalecer la cultura de seguridad, garantizar la protección de los activos de información y promover un entorno confiable, resiliente y conforme al marco normativo nacional.

8.2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Jardín Botánico de Bogotá José Celestino Mutis (JBJCM) reconoce la importancia estratégica de sus activos de información para el cumplimiento de su misión institucional y la adecuada prestación de sus servicios a la ciudadanía y al Distrito Capital. En este sentido, la Entidad reafirma su compromiso con la implementación, operación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), orientado a proteger la confidencialidad, integridad, disponibilidad y privacidad de la información en todas sus formas.

Este compromiso se materializa mediante la gestión sistemática de los riesgos de seguridad de la información, la adopción de controles organizacionales, técnicos y operativos que permitan mitigar amenazas y vulnerabilidades, y el fortalecimiento de un entorno de confianza que respalde el ejercicio de la misión institucional bajo los más altos estándares de seguridad digital. Todas estas acciones se desarrollan en estricto cumplimiento del marco normativo vigente aplicable a las entidades públicas del Estado colombiano.

Los lineamientos específicos que orientan la Seguridad y Privacidad de la Información del JBJCM están definidos en el documento SDI.PR.01.M.02 – Manual de Políticas Específicas del MSPI, el cual es de obligatorio cumplimiento para funcionarios, contratistas, proveedores, usuarios con acceso autorizado y visitantes que interactúen con los activos de información de la Entidad. Dicho manual establece directrices relacionadas con:

- **Seguridad en los recursos humanos:** Establece medidas antes, durante y después de la vinculación laboral, tales como la verificación de antecedentes, la firma de acuerdos de confidencialidad, la aceptación expresa de las políticas de seguridad y la socialización de responsabilidades. Busca asegurar que todas las personas que interactúan con activos de información comprendan su rol y actúen conforme a la normativa vigente.
- **Seguridad en la gestión de activos:** Reconoce como propiedad institucional toda la información y los recursos tecnológicos generados, administrados o utilizados en el marco de las funciones del JBJCM. La Entidad mantiene un inventario actualizado y clasificado de activos de información, regulando su uso, custodia, tratamiento y disposición final exclusivamente para fines institucionales.
- **Gestión de Vulnerabilidades:** Establece los lineamientos para la identificación, análisis, priorización, tratamiento y seguimiento de las vulnerabilidades presentes en los sistemas, aplicaciones, infraestructuras, dispositivos y servicios del JBJCM. Incluye la ejecución periódica

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 10 de 14	

de análisis de vulnerabilidades, la evaluación del impacto asociado, la verificación de exposiciones técnicas (como CVE y CVSS), la aplicación oportuna de parches y actualizaciones, y la implementación de controles de mitigación cuando no sea posible actualizar de inmediato.

- **Control de acceso lógico:** Define mecanismos de autenticación, autorización, segregación de funciones y gestión de credenciales que permitan prevenir el acceso no autorizado a sistemas, redes, aplicaciones y bases de datos, garantizando la trazabilidad y el principio de mínimo privilegio.
- **Criptografía:** Regula el uso de técnicas y herramientas de cifrado para proteger la información en reposo y en tránsito, así como la gestión segura del ciclo de vida de las claves criptográficas, de acuerdo con estándares internacionales y la normativa vigente.
- **Seguridad física y del entorno:** Establece controles para proteger las instalaciones, áreas seguras y equipos institucionales frente a accesos físicos no autorizados, desastres, fallas ambientales y demás riesgos que puedan afectar la confidencialidad, la integridad o la disponibilidad de los activos de información.
- **Seguridad en las operaciones:** Comprende la planificación, ejecución y monitoreo de las actividades operativas del área tecnológica, incluyendo controles de cambios, gestión de configuraciones, registros de auditoría, respaldo, monitoreo continuo, protección antimalware y demás procedimientos que aseguren una operación estable y confiable.
- **Seguridad de las comunicaciones:** Regula la protección de redes internas y externas, la transferencia segura de información, la segregación de redes, el uso de VPN, el cifrado en las comunicaciones y el cumplimiento de acuerdos de niveles de servicio, garantizando la integridad y disponibilidad de los datos transmitidos.
- **Seguridad para dispositivos móviles:** Define controles para el uso, configuración, protección, almacenamiento y conexión de dispositivos móviles institucionales, minimizando su exposición a amenazas externas y asegurando la protección de la información que pueda residir en ellos o transitar por ellos.
- **Adquisición, desarrollo y mantenimiento de sistemas:** Garantiza que todos los sistemas de información, desde su diseño y adquisición, hasta su desarrollo, pruebas, despliegue y mantenimiento, incluyan requisitos de seguridad alineados con el MSPI. Promueve los principios de seguridad por diseño, de seguridad por defecto y de revisión continua de vulnerabilidades.
- **Relaciones con proveedores:** Exige que los contratos, acuerdos de nivel de servicio y convenios incluyan obligaciones de seguridad, cláusulas de confidencialidad, protección de datos, niveles de servicio y requisitos para el manejo seguro de información y de servicios tercerizados.
- **Seguridad de la información en la continuidad del negocio:** Incorpora medidas de continuidad operacional y recuperación tecnológica (DRP y BCP), así como análisis de impacto al negocio (BIA), con el fin de asegurar la disponibilidad de los servicios críticos ante incidentes, fallas, desastres o interrupciones.
- **Gestión de incidentes de seguridad de la información:** Establece los procedimientos para la detección, el reporte, el análisis, el tratamiento, el registro y el cierre de incidentes de seguridad. La Oficina de Sistemas coordina la respuesta, mientras que todos los usuarios están obligados a reportar oportunamente cualquier anomalía o incidente.
- **Seguridad en la nube:** Define los requisitos para la adopción y el uso seguros de servicios en la nube, considerando aspectos como la ubicación de los datos, acuerdos de servicio, medidas de seguridad implementadas por el proveedor, contingencias, protección de datos personales y cumplimiento normativo.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 11 de 14	

- **Inteligencia Artificial:** Establece directrices para el diseño, desarrollo, adopción y uso responsable de soluciones basadas en inteligencia artificial, asegurando la transparencia, la trazabilidad, la seguridad, la privacidad y la protección de los datos utilizados por estos sistemas, conforme a la normativa vigente y a los principios éticos aplicables.
- **Cumplimiento:** Asegura la observancia de las leyes, regulaciones, estándares y políticas aplicables en materia de seguridad digital, protección de datos personales, acceso a la información pública, uso de tecnología institucional, contraseñas seguras, mantenimiento de escritorios limpios y otras exigencias normativas.
- **BYOD (Bring Your Own Device / Dispositivos Propios):** Regula el uso de dispositivos personales para actividades laborales, estableciendo controles técnicos y organizacionales que protejan la información institucional, garanticen la separación entre datos corporativos y personales, y eviten fugas o pérdidas de información.
- **Trabajo remoto y teletrabajo:** Define los requisitos, medidas de seguridad y controles mínimos para el acceso remoto seguro a sistemas y datos institucionales, garantizando la confidencialidad, integridad y disponibilidad de la información desde ubicaciones externas.
- **Respaldo de información (Backups):** Establece los procedimientos para la generación, almacenamiento, verificación y restauración de copias de seguridad, asegurando que la información crítica pueda recuperarse ante fallas técnicas, incidentes de seguridad, errores humanos o desastres.
- **Transferencia de información:** Regula los mecanismos, formatos y canales autorizados para la transferencia interna y externa de información, garantizando que toda transmisión se realice de manera segura, cifrada cuando corresponda, minimizando los riesgos de interceptación, pérdida o manipulación no autorizadas y asegurando la protección de los datos personales y sensibles.

Estos lineamientos deben integrarse en los procedimientos, manuales, instructivos y formatos de los procesos de la Entidad que correspondan, en especial en aquellos relacionados con la implementación de controles de Seguridad de la Información, la Gestión de Tecnología, la Gestión Documental y demás procesos que administren activos de información o soporten servicios institucionales.

La implementación de la Política de Seguridad y Privacidad de la Información se evidencia mediante la Matriz de Evaluación, Aplicabilidad y Diagnóstico de Controles - SDI.PR.02.F.02, una herramienta que permite verificar el cumplimiento de los requisitos del MSPI y la efectividad de los controles implementados.

Las actividades necesarias para garantizar la correcta operación del Modelo se desarrollan a través de los siguientes planes, alineados al proceso de seguridad y privacidad de la información:

- SDI.PLA.02 Plan de Seguridad y Privacidad de la Información
- SDI.PLA.03 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- SDI.PLA.01. Plan de Sensibilización de Seguridad, Privacidad de la Información y Protección de Datos Personales -

8.3. APLICABILIDAD

La presente Política de Seguridad y Privacidad de la Información, sus objetivos, lineamientos y toda la documentación derivada o complementaria —incluyendo planes, procedimientos, instructivos, guías,

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 12 de 14	

manuales y controles asociados— aplican a toda la Entidad, sin excepción. Es de obligatorio cumplimiento para:

- Funcionarios, contratistas, consultores y personal en misión del JBJCM.
- Proveedores y terceros que presten servicios o participen en actividades que involucren activos de información.
- Usuarios internos o externos que accedan, gestionen, procesen o utilicen información del JBJCM bajo cualquier modalidad.

La aplicabilidad se extiende a toda la información administrada por la Entidad, sin importar su forma, medio, soporte, ubicación o sistema en el que repose, y a todos los procesos misionales, estratégicos, de apoyo y de evaluación.

8.4. SANCIONES

El incumplimiento de la Política de Seguridad y Privacidad de la Información del JBJCM constituye una falta que puede acarrear consecuencias disciplinarias, contractuales, administrativas, civiles y penales, conforme al ordenamiento jurídico colombiano.

Las sanciones se aplicarán de acuerdo con:

- Las normas y procedimientos establecidos en la legislación colombiana, incluido el régimen disciplinario aplicable a los servidores públicos.
- Las cláusulas contractuales suscritas con contratistas y proveedores.
- El Código Penal colombiano, particularmente las disposiciones relacionadas con los delitos informáticos y la protección de datos.

Las políticas internas del JBJCM, incluyendo normas sobre el uso de recursos, la confidencialidad, el tratamiento de datos personales y la seguridad digital.

La severidad de la sanción dependerá de la gravedad de la falta, del impacto generado, del nivel de afectación a los activos de información, de la reincidencia y de la intencionalidad del infractor.

8.5. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL MSPI

El Jardín Botánico José Celestino Mutis (JBJCM) realizará revisiones periódicas, de manera anual y sistemáticas del Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de evaluar su desempeño, eficacia y nivel de cumplimiento de los requisitos normativos, institucionales y de seguridad digital.

Estas revisiones se desarrollarán de acuerdo con las responsabilidades establecidas y estarán orientadas a los siguientes aspectos:

- **Oficial de Seguridad de la Información:** Responsable del seguimiento continuo de la gestión del riesgo de seguridad de la información, de la gestión de incidentes, del estado de implementación de los controles y, en general, de la operación del MSPI dentro de la Entidad.
- **Oficina Asesora de Planeación:** Encargada de realizar el seguimiento cuatrimestral de los indicadores de desempeño del Proceso de Seguridad de la Información, evaluando el cumplimiento de las metas, la efectividad de los controles y la evolución del modelo.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				 BOGOTÁ
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 13 de 14	

- **Comité Institucional de Gestión y Desempeño:** Revisa semestralmente el avance de la Política de Seguridad Digital y del MSPI, de acuerdo con los lineamientos del FURAG o con la herramienta que se defina para medir la gestión institucional en materia de gobierno digital y seguridad.
- **Oficina de Control Interno:** Brinda asesoría coordinada con la Oficina Asesora de Planeación a la primera línea de defensa, orientando sobre situaciones que puedan afectar el cumplimiento de la política e identificando oportunidades de mejora en los controles, procesos y prácticas asociados a la seguridad y la privacidad de la información.

Los resultados de estas revisiones generarán acciones de mejora continua, orientadas a disminuir las brechas de cumplimiento, fortalecer los controles existentes y garantizar la evolución permanente del MSPI conforme a los riesgos, las necesidades institucionales y los cambios normativos.

8.6. REVISIÓN Y VIGENCIA

Revisión: La presente Política de Seguridad y Privacidad de la Información será revisada anualmente o cuando se produzcan cambios normativos, tecnológicos u organizacionales que así lo ameriten. El proceso de revisión estará a cargo de la Oficina Asesora de Planeación, o de la dependencia o del funcionario que sea designado para tal fin, quien deberá evaluar la pertinencia, vigencia y suficiencia de los lineamientos establecidos, proponiendo los ajustes necesarios para su actualización y mejora continua.

Vigencia: La presente política fue adoptada mediante la Resolución 168 del 31 de mayo de 2023 y rige a partir de la fecha de su expedición, manteniéndose vigente hasta que sea formalmente modificada, actualizada o derogada mediante el acto administrativo correspondiente.

 ALCALDÍA MAYOR DE BOGOTÁ D.C.	JARDÍN BOTÁNICO	MANUAL DE PROCESOS Y PROCEDIMIENTOS				
		SDI – SEGURIDAD DE LA INFORMACIÓN				
		Política: Seguridad y Privacidad de la Información				
		Código: SDI.PO.01	Versión: 4	Fecha: 17/12/2025	Página: 14 de 14	

9. BIBLIOGRAFIA

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements. <https://www.iso.org/standard/82875.html>
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Modelo de Seguridad y Privacidad de la Información – MSPI (versión 5). https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Resolución 2277 de 2025. https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_2277_2025.htm.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021). Resolución 500 de 2021. <https://gobiernodigital.mintic.gov.co/portal/604/w3-article-153204.html>
- Departamento Nacional de Planeación (DNP). (2020). [Política Nacional de Confianza y Seguridad Digital. Documento CONPES 3995.](#)

10. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
12/09/2019	1	Se ajusta y adopta la Política General de Seguridad.
15/12/2021	2	Se actualiza la Política General de Seguridad y Privacidad de la Información.
30/04/2023	3	Se ajusta por observaciones de auditoría de Control Interno.
17/12/2025	4	Se actualiza la Política General de Seguridad y Privacidad de la Información por la nueva versión de MSPI y observaciones de la Oficina de Control Interno mediante comité No 10 del 11 de diciembre 2025. Se ajusta Normatividad, Principios, Roles, Marco Conceptual, Organización de la seguridad de la información, Ruta de implementación.

11. AUTORIZACIONES

PROCESO						
ELABORÓ			APROBÓ			
Nombre(s):	Paola Ambrosio		Nombre(s):	Sandra Marcela Torres		
Cargo(s):	Contratista Oficina Asesora de Planeación		Cargo(s):	Jefe Oficina Asesora Planeación		
OFICINA ASESORA DE PLANEACIÓN						
REVISÓ			APROBÓ		PUBLICÓ	
Nombre(s):	José David Hernández M.		Nombre(s):	Sandra Marcela Torres	Nombre(s):	José David Hernández M.
Cargo(s):	Contratista MIPG - SIG Oficina Asesora de Planeación		Cargo(s):	Jefe Oficina Asesora Planeación	Cargo(s):	Contratista MIPG - SIG Oficina Asesora de Planeación