

**PLAN DE SEGURIDAD Y PRIVACIDAD DE  
LA INFORMACIÓN - SEGURIDAD DIGITAL**



**OFICINA ASESORA DE PLANEACIÓN**

**2024**





**JARDÍN BOTÁNICO  
DE BOGOTÁ**

**BOGOTÁ**

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Múts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 1 de 21	

## CONTENIDO

1.	INTRODUCCIÓN .....	2
2.	OBJETIVO .....	3
3.	OBJETIVOS ESPECÍFICOS.....	3
4.	ALCANCE .....	3
5.	NORMATIVIDAD .....	4
6.	MARCO CONCEPTUAL .....	6
7.	ALINEACIÓN A POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON LAS POLÍTICAS DE USO DE LA INFORMACIÓN Y DATOS PERSONALES...	8
8.	GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	9
8.1.	PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	12
8.2.	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ACTUALIZACIÓN MEDIANTE RESOLUCIÓN 168 DE 2023) Y POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (ACTUALIZACIÓN MEDIANTE RESOLUCIÓN 349 DE 2023).....	13
8.3.	OJETIVOS DE LAS POLITICAS.....	14
8.4.	METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DEL INFORMACIÓN- MSPI.....	15
8.5.	PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	15
8.6.	MEDICION .....	20
9.	CONTROL DE CAMBIOS.....	20
10.	AUTORIZACIONES: .....	20

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				 <p>BOGOTÁ   JARDÍN BOTÁNICO DE BOGOTÁ</p>
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 2 de 21	



## 1. INTRODUCCIÓN

El Jardín Botánico de Bogotá “José Celestino Mutis”, mediante la Resolución 161 del 30 de mayo de 2023, “Por la cual se conforma y establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño del Jardín Botánico de Bogotá José Celestino Mutis y se deroga las resoluciones No. 411 de 2018 y la No. 289 de 2020 y se dictan otras disposiciones”, en su artículo 5, entre las funciones del Comité Institucional de Gestión y Desempeño”, se encuentra en el ítem 8, Asegurar la implementación y el desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. Igualmente, mediante el su artículo 11: Adoptar los lineamientos establecidos en las Políticas de Gestión y Desempeño Institucional, de que trata el artículo 2.2.22.2.1 del Decreto 1083 de 2015. Modificado por el Decreto 1299 de 2018, se tiene la de Seguridad digital. Igualmente, el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera el Decreto 767 de 2022 en el artículo 2.2.9.1.2.1 define la estructura a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. Así mismo, el numeral 3.2 del mismo artículo define la Seguridad y Privacidad de la Información como habilitador que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos; en el mismo sentido el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el párrafo del artículo 16 indica que (...)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones(...). En cumplimiento de este Decreto se emite la Resolución 500 de 2021<sup>1</sup>, expedida por el MinTIC, estableció los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del modelo de seguridad y privacidad -MSPI<sup>2</sup>, como habilitador de la política de Gobierno Digital. En consecuencia, la seguridad y privacidad de la información, y el Modelo de Seguridad y Privacidad de la Información será adoptada en el Jardín Botánico José Celestino Mutis en adelante (JBB).

Dando cumplimiento a la normativa anterior, El Jardín Botánico de Bogotá, ha adelantado cambios organizacionales para orientar estratégicamente sus actividades con el apoyo de Gestión de las tecnologías de la información, infraestructura tecnológica y las comunicaciones, por lo cual se actualiza el presente documento Plan de Seguridad y Privacidad de la Información - Seguridad Digital; que establece los detalles de cómo se realizará la implementación y mejora de la seguridad de la información en la Entidad para cada vigencia, estipulando directrices, tiempos y responsables, de tal forma que se logren resultados anuales, y siendo aprobado por comité del Modelo Integrado de Gestión del 24 de enero de 2024, dando cumplimiento a lo establecido en el Decreto 612 de 2018,

<sup>1</sup> [articles-162624\\_recurso\\_1.pdf \(mintic.gov.co\)](#)

<sup>2</sup> [articles-162623\\_recurso\\_1.pdf \(mintic.gov.co\)](#)

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 3 de 21	

## 2. OBJETIVO



Establecer acciones para fortalecer Seguridad y Privacidad de la Información- Seguridad Digital, en el Jardín Botánico José Celestino, mediante la planeación de actividades para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua de la Seguridad y Privacidad de la Información en la Entidad, las cuales se encuentran alineadas con la con el estándar (NTC-ISO/IEC 27001), la Política pública de Seguridad Digital , el Modelo de Seguridad y Privacidad de la Información- MSPI, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC y Metodología para la implementación del Modelo de Seguridad y Privacidad del Información- MSPI en el JBB, que permitan mantener la seguridad y privacidad de la información en la aplicación del proceso SDI- Seguridad de la Información.

## 3. OBJETIVOS ESPECÍFICOS

- ✓ Determinar las acciones a realizar en el Jardín Botánico de Bogotá (JBB) durante el diagnóstico, planificación, operación, evaluación y mejoramiento del Modelo de Seguridad y Privacidad - MSPI en cuanto al cumplimiento como entidad de diseñar, implantar y mantener actualizada la seguridad digital a partir de los activos a proteger y de los riesgos a que están sometidos.
- ✓ Promover una cultura de seguridad y privacidad de la información entre todo el personal del Jardín Botánico, con el fin de proteger adecuadamente los activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y cumplir con las regulaciones y estándares pertinentes en el cumplimiento de las medidas de seguridad digital a partir de la construcción de estrategias de comunicación y sensibilización que divulguen las directrices, políticas y beneficios de la Seguridad Digital a los funcionarios, contratistas y terceros en el JBB.
- ✓ Detectar, informar, evaluar, responder, minimizar, aprender y resolver incidentes de seguridad de la información con el propósito de realizar una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de los activos de información el Jardín Botánico José Celestino Mutis-JBB.
- ✓ Identificar y gestionar activos de seguridad digital y de la información para los procesos del Jardín Botánico de Bogotá José Celestino Mutis, como ejercicio fundamental para la gestión de Riesgos de Seguridad Digital, así como la valoración e implementación de controles con el fin de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la Entidad.
- ✓ Establecer los principios y lineamientos que deben regir el tratamiento de los datos personales dentro del Jardín Botánico José Celestino Mutis. Esto incluye la recolección, almacenamiento, uso, divulgación y disposición de los datos personales, asegurando que se realicen de manera legal, transparente, y respetando los derechos de los titulares de los datos

## 4. ALCANCE

El presente documento se aplica para todos los procesos del Jardín Botánico de Bogotá (JBB) a todos los funcionarios, contratistas y demás colaboradores que en cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, este plan aplica para toda la información

	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 4 de 21	

creada, procesada o utilizada en la Entidad sin importar el medio, formato, presentación o lugar en el cual se encuentre, dando cumplimiento a lo establecido en el Decreto 612 de 2018, a la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información alineado con estándar (NTC-ISO/IEC 27001), así como la estrategia de Seguridad Digital del Estado colombiano.

## 5. NORMATIVIDAD

La Constitución Política de Colombia en su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.



Que los artículos 209 y 269 de la Constitución Política han señalado que la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley. Por ello, las autoridades de las entidades públicas están en la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El artículo 17 de la Ley Estatutaria 1581 de 2012, "Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

La Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

Ley 1952 del 2019 por la cual se expide el código general disciplinario que deroga la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario. Artículo 38 deberes. son deberes de todo servidor público: "5. utilizar los bienes y recursos asignados para el desempeño de su empleo cargo función, las facultades que les sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines que están afectos. 6. custodiar y cuidar la documentación e información que, por razón de su empleo, cargo función conserve bajo su cuidado OA la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Múts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 5 de 21	

El artículo 2.2.9.1.1.3. del Decreto 1078 de 2015. subrogado por el artículo 1 del Decreto 1008 de 2018. determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través de este se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

ARTÍCULO 2.2.9.1.2.1. del decreto 767 del 2022 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del

Decreto 612 de 2018. 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 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones que dentro de la estructura tiene el 3.2 Seguridad y Privacidad de la Información: como habilitador que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Que en el artículo 2.2.22.3.2. del Decreto 1083 de 2015, se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el "Marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan /as necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

Que mediante el artículo 1 del Decreto 1499 de 2017, se sustituyó el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015. El nuevo artículo 2.2.22.1.1 del Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", señala que el Sistema de Gestión "que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad".

La Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y. establece los lineamientos y

	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 6 de 21	

estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

El artículo 5 de la misma Resolución establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información - MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

El Documento CONPES 3854 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El Documento CONPES 3995 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías. A su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.



Directiva 011 de 2023. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

## 6. MARCO CONCEPTUAL

A continuación, se listan algunas de los conceptos más importantes, relacionados 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).
- **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.)



Verificar su vigencia en el Listado Maestro de Documentos

	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 7 de 21	

que tenga valor para la organización. (Modelo de Seguridad y Privacidad de la Información, 2021).

- **Amenaza:** Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).
- **Análisis de riesgos:** Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo. (Modelo de Seguridad y Privacidad de la Información, 2021).
- **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).
- **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).
- **Entrenamiento:** Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo. Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación. (Plan de Capacitación, 2016)
- **Gestión de incidentes de seguridad de la información:** Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (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 de la información:** único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información, (ISO/CEI 27000, 2018).
- **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 complejidad de la información. (ISO/CEI 27000, 2018).



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 8 de 21	



- **Parte interesada (Stakeholders):** 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, 2021).
- **Riesgo:** La posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización. (ISO/CEI 27000, 2018).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/CEI 27000, 2018).
- **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) 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).
- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular (Plan de Capacitación, 2016)
- **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).

Que la adopción del modelo de seguridad de la información (MSPI), es una decisión estratégica para una organización. El establecimiento e implementación del modelo de seguridad de la información de una entidad pública como es el JBB, están influenciados por las necesidades y objetivos de la Entidad, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

## 7. ALINEACIÓN A POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON LAS POLÍTICAS DE USO DE LA INFORMACIÓN Y DATOS PERSONALES

El plan de seguridad de la información está alineado con la Resolución 168 de 31 de mayo del 2023<sup>3</sup>

<sup>3</sup>[https://jbb.gov.co/documentos/juridica/2023/168-2023\\_Actualizacion\\_Politica\\_de\\_Seguridad\\_de\\_la\\_Informacion\\_rev\\_\(CFMP-GOF-CRS\)%2001.06.2023.pdf](https://jbb.gov.co/documentos/juridica/2023/168-2023_Actualizacion_Politica_de_Seguridad_de_la_Informacion_rev_(CFMP-GOF-CRS)%2001.06.2023.pdf)

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 9 de 21	

“Por medio de la cual se actualiza la Política General de Seguridad y Privacidad de la Información del Jardín Botánico José Celestino Mutis”, en la medida que permite la participación de los funcionarios, contratistas y terceros en lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de seguridad de la información (tendrán la responsabilidad de divulgar y sensibilizar las políticas y procedimientos de seguridad y privacidad de la información). Así mismo la política y lineamientos expuestos en el “Manual de normas y políticas de seguridad y privacidad de la información”, son de obligatorio cumplimiento para los funcionarios y contratistas de la entidad. En el caso de cualquier sugerencia de cambio o normatividad actualizada se tramitará a través de la Oficina de Tecnologías de la Información, quien se encargará de realizar el cambio y socialización en la Entidad.

Así mismo el JBB, está comprometido en garantizar el tratamiento de los datos personales, por lo cual se acoge a las disposiciones contenidas en la Ley 1581 de 2012 y su Resolución 349<sup>4</sup> Por la cual se deroga la resolución 412 de 2019 y se adopta la Política de Tratamiento de Datos Personales del Jardín Botánico de Bogotá José Celestino Mutis.

## 8. GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Respecto a los resultados del MSPI del año 2023, se encontró que para la vigencia 2024 es necesario atender las siguientes recomendaciones:

- ✓ Fortalecer participación en la mejora de las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del de seguridad digital convocadas por el JBB
- ✓ Adelantar acciones para la gestión sistemática de los riesgos de seguridad digital en la entidad tales como gestión de vulnerabilidades.
- ✓ Adelantar acciones para la gestión de la continuidad de los servicios de infraestructura tecnológica.
- ✓ Comprometer la seguridad de la información con los proveedores internos y externos.

Adicionalmente, en el análisis de brechas del Modelo de Seguridad y Privacidad de la Información – MSPI realizado en 2023, se obtuvo el 76% avance dentro del Evaluación y efectividad de los controles y un avance ciclo de funcionamiento del modelo de operación (PHVA) del 82% siguiente resultado:



<sup>4</sup> [https://jbb.gov.co/documentos/juridica/2023/349-2023\\_Resolucion\\_Adopcion\\_Politica\\_Datos\\_personales.pdf](https://jbb.gov.co/documentos/juridica/2023/349-2023_Resolucion_Adopcion_Politica_Datos_personales.pdf)

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	<b>OPTIMIZADO</b>
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	100	<b>OPTIMIZADO</b>
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	97	100	<b>OPTIMIZADO</b>
A.8	GESTIÓN DE ACTIVOS	76	100	<b>GESTIONADO</b>
A.9	CONTROL DE ACCESO	78	100	<b>GESTIONADO</b>
A.10	CRIPTOGRAFÍA	80	100	<b>GESTIONADO</b>
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	72	100	<b>GESTIONADO</b>
A.12	SEGURIDAD DE LAS OPERACIONES	69	100	<b>GESTIONADO</b>
A.13	SEGURIDAD DE LAS COMUNICACIONES	60	100	<b>EFFECTIVO</b>
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	<b>EFFECTIVO</b>
A.15	RELACIONES CON LOS PROVEEDORES	60	100	<b>EFFECTIVO</b>
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	<b>GESTIONADO</b>
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	<b>EFFECTIVO</b>
A.18	CUMPLIMIENTO	84	100	<b>OPTIMIZADO</b>
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>76</b>	<b>100</b>	<b>GESTIONADO</b>

*Ilustración 1 Evaluación de Efectividad de controles Autodiagnóstico MinTIC*



*Ilustración 2 brecha anexo a ISO 27001:2013*

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Múts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				 <p>BOGOTÁ   JARDÍN BOTÁNICO DE BOGOTÁ</p>
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 11 de 21	



AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	36%	40%
Implementación	15%	20%
Evaluación de desempeño	16%	20%
Mejora continua	16%	20%
<b>TOTAL</b>	<b>82%</b>	<b>100%</b>

Ilustración 3 Avance ciclo de funcionamiento del modelo de operación (PHVA)

De la gráfica anterior, se identifican aspectos por mejorar en los siguientes controles de seguridad de la información.

ITEM	DESCRIPCION	Control ISO 27002: 2013 / 27002: 2022
<b>ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</b>	<p>Elaborar Plan de continuidad del negocio que deben desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos comerciales críticos luego de una interrupción o falla. La seguridad de la información debe restaurarse al nivel requerido y en los plazos requeridos.</p> <p>Así mismo se debe actualizar el análisis de impacto empresarial (BIA), elaborar e implementar el plan de pruebas de restauración.</p>	<p>A. 17.1.1 - 17.1.2 17.1.3 5.29 - 8.14</p>
<b>RELACIONES CON LOS PROVEEDORES</b>	<p>Contar con alternativas de acuerdos con los proveedores deben establecerse y documentarse para garantizar que haya un entendimiento claro entre la organización y el proveedor con respecto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes</p> <p>El seguimiento, la revisión y la gestión de cambios de los servicios del proveedor deben garantizar que se cumplan los términos y condiciones de seguridad de la información de los acuerdos, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente y que los cambios</p>	<p>A 15.1.1 -15.1.2-15.1.3-15.2.1-15.2.2 5.19- 5.20- 5.21-5.22</p>

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				 <p>BOGOTÁ JARDÍN BOTÁNICO DE BOGOTÁ</p>
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 12 de 21	

	en los servicios del proveedor o el estado comercial no afecten la prestación del servicio.	
<b>SEGURIDAD DE LAS COMUNICACIONES</b>	Se deben implementar controles para garantizar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado. En particular, se deben considerar documentar Seguridad de redes, Seguridad de los servicios de red y Segregación de redes, adicionalmente las políticas de navegación de la Entidad.	A 13.2.1- 13.2.2 -13.2.3-13.2.4-13.1.1 -13.1.2-13.1.3 5.14-6.6-8.20-8.218.22
<b>ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS</b>	Fortalecer el desarrollo seguro que es un requisito para crear un servicio, una arquitectura, un software y un sistema seguro con la solicitud de Pruebas de seguridad en desarrollo y aceptación, así los diagramas de arquitecturas de los sistemas de información internos y externos documentados , así como las integración de bases de datos para su protección.	A 14.2.1 -14.1.2, 14.1.3 -14.2.5 -14.2.8 -14.2.9- 14.2.714.3.1 8.25-8.26-8.27-8.29-8.30-8.33

## 8.1. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Jardín Botánico de Bogotá llevó diversas actividades orientadas a la implementación y fortalecimiento del Sistema Integrado de Gestión en la entidad. Las acciones realizadas están alineadas con los requisitos de las Normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018, así como con los lineamientos de las Políticas y Lineamientos de MIPG.

El modelo de operación actual de JBB se encuentra orientado mediante la gestión de procesos, y se representan en la siguiente ilustración:



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>			
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>			
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>			
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	



Ilustración 4 Mapa de procesos JBB



Los Procesos de la entidad se encuentran alineados al sistema integrado de gestión donde se encuentran agrupados y representados en el mapa de procesos. Se contempló el proceso Estratégico de Seguridad de la Información - **SDI**, que tiene como objetivo; Proteger la disponibilidad, integridad y confidencialidad de los activos de información en el Jardín Botánico de Bogotá José Celestino Mutis, a través de la gestión de riesgos de seguridad y privacidad de la información y la implementación de políticas, procedimientos y controles necesarios y suficientes, de manera que se puedan prevenir y gestionar los incidentes de seguridad de la información y violaciones de privacidad contribuyendo al cumplimiento de la misión institucional y los objetivos estratégicos.

## 8.2. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ACTUALIZACIÓN MEDIANTE RESOLUCIÓN 168 DE 2023) Y POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (ACTUALIZACIÓN MEDIANTE RESOLUCIÓN 349 DE 2023).

Por medio [Resolución 168](#) del 30 de mayo de 2023, se actualiza la Política General de Seguridad y Privacidad de la Información del Jardín Botánico José Celestino Mutis.

Esta Política General de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Jardín Botánico José Celestino Mutis con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del proceso de Seguridad de la Información (SDI), por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

De la misma manera, Por medio [Resolución 349](#) del 13 de octubre del 2023, se deroga la resolución 412 de 2019 y se adopta la Política de Tratamiento de Datos Personales del Jardín Botánico de Bogotá José Celestino Mutis

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 14 de 21	

Esta Política tiene como objetivo principal proporcionar la información necesaria a los distintos grupos de interés y establecer los lineamientos que aseguren la protección de los datos personales que son objeto de tratamiento por parte del Jardín Botánico José Celestino Mutis. A través de esta política, la entidad se compromete a cumplir con la legislación vigente, así como con las políticas y procedimientos establecidos para garantizar los derechos de los titulares de los datos. Además, se establecen criterios claros sobre la recolección, almacenamiento, uso, circulación y supresión de los datos personales, en cumplimiento de los estándares de privacidad y seguridad establecidos.

### 8.3. OBJETIVOS DE LAS POLITICAS



Objetivo general de la Política de seguridad de la Información es establecer los lineamientos definidos por la Dirección de Jardín Botánico José Celestino Mutis para la seguridad de la información, teniendo en cuenta la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

Con los siguientes objetivos específicos:

- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información. → Minimizar el riesgo de todos los procesos de la entidad.
- ✓ Mejorar continuamente la gestión de seguridad de la información en el MSPI.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y grupos de interés y de valor en el Jardín Botánico José Celestino Mutis, para los activos de seguridad digital.
- ✓ Implementar los controles tecnológicos necesarios para la protección de los activos en el Jardín Botánico José Celestino Mutis y para la reducción de los riesgos.

Objetivo principal de la Política de Tratamiento de Datos Personales es proporcionar la información necesaria a los distintos grupos de interés y establecer los lineamientos que aseguren la protección de los datos personales que son objeto de tratamiento por parte del Jardín Botánico José Celestino Mutis. A través de esta política, la entidad se compromete a cumplir con la legislación vigente, así como con las políticas y procedimientos establecidos para garantizar los derechos de los titulares de los datos. Además, se establecen criterios claros sobre la recolección, almacenamiento, uso, circulación y supresión de los datos personales, en cumplimiento de los estándares de privacidad y seguridad establecidos.

- ✓ Proteger la privacidad de los visitantes, empleados y colaboradores
- ✓ Establecer los principios y lineamientos que deben regir el tratamiento de los datos personales dentro del Jardín Botánico José Celestino Mutis.
- ✓ Generar confianza y tranquilidad en las personas e instituciones que interactúan con la Entidad, al establecer principios claros de privacidad y seguridad, así como al informar de manera transparente sobre las prácticas de tratamiento de datos, se busca fomentar la confianza y
- ✓ Promover una relación sólida con los visitantes, empleados y colaboradores.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Mutis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 15 de 21	

- ✓ Proteger los datos personales contra cualquier riesgo de acceso no autorizado, pérdida, alteración, divulgación o destrucción. Se establecen medidas técnicas, administrativas y organizativas adecuadas para proteger la seguridad de los datos y minimizar los riesgos asociados al tratamiento de la información personal, para lo cual se articulará con la Política de Seguridad de la Información del Jardín Botánico José Celestino Mutis.

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros del Jardín Botánico José Celestino Mutis y el incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa vigente.

#### 8.4. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DEL INFORMACIÓN- MSPI.

Con la implementación del MSPI se plateo una metodología para determinar las acciones a realizar en el Jardín Botánico de Bogotá (JBB) durante el diagnóstico, planificación, operación, evaluación y mejoramiento del Modelo de Seguridad y Privacidad - MSPI en cuanto al cumplimiento como entidad de diseñar, implantar y mantener actualizada la seguridad digital a partir de los bienes a proteger y de los riesgos a que están sometidos, a través de documento guía, SDI.PR.02.G.02 Metodología de implementación del Modelo de Seguridad y Privacidad.



#### 8.5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación de Seguridad y Privacidad de la Información, para la aplicación del habilitador de seguridad de la información de la política de gobierno digital, se proyecta con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información de JBB y se ejecuta de acuerdo con el siguiente cronograma, al cual se le hace seguimiento por parte de oficial de Seguridad de información y el Plan de Acción Institucional.

FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
<b>DIAGNOSTICO MSPI</b>	Actualizar el documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad	01-01-2024	30-12-2024	Documento autodiagnóstico de MSPI actualizado semestralmente	Oficina Asesora de Planeación Oficial de seguridad de Información
<b>PLANIFICACION SDI</b>	Actualizar el Plan de Seguridad y Privacidad de la Información con su respectivo Alcance	01-01-2024	30-01-2024	Documento Plan de Seguridad y Privacidad de la Información –	Oficina Asesora de Planeación



Verificar su vigencia en el Listado Maestro de Documentos



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 16 de 21	



FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
	MSPI, asociadas a la seguridad Digital			Seguridad Digital 2024	Oficial de seguridad de Información
	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	01-01-2024	30-01-2024	Documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información- Seguridad Digital 2024	Oficina Asesora de Planeación  Oficial de seguridad de Información
	Definir una metodología de pruebas de efectividad JBB	01-03-2024	30-04-2024	Documento guía metodología de pruebas de efectividad JBB – Infraestructura tecnológica	Oficina Asesora de Planeación  Secretaria General - Sistemas
	Revisión anual de la Política de seguridad y privacidad de la información.	1-04-2024	30-05-2024	Acta de revisión de la política de seguridad y privacidad de la información y/o Resolución de actualización	Oficina Asesora de Planeación  Oficial de seguridad de Información
	Actualizar el Análisis de Impacto de la Operación.	1-03-2024	30-05-2024	Documento Actualizado del Análisis de Impacto del Negocio BIA. Documento	Secretaria General - Sistemas
	Actualizar la gestión de Continuidad del Negocio de JBB	1-03-2024	30-05-2024	Documento Actualizado Plan de Continuidad del Negocio de JBB alineado al proceso de gestión e la tecnología	Secretaria General - Sistemas
	Implementar la Primera Fase del DRP con los recursos tecnológicos disponibles en el JBB	1-06-2024	30-09-2024	Documento actualizado del Plan DRP y generar los scripts de activación	Secretaria General - Sistemas
	Definir el plan de pruebas de la infraestructura tecnológica de JBB, incluida en la primera fase del DRP	1-09-2024	30-11-2024	Documento plan de pruebas de restauración de la infraestructura tecnológica de JBB, incluidas las pruebas de los scripts de activación	Secretaria General - Sistemas

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 17 de 21	



FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
<b>OPERACION SDI</b>	Realizar la Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	30-01-2024	15-03-2024	Actualizar la matriz Mapa de Riesgos Sistema Seguridad de la Información	Oficina Asesora de Planeación Oficial de seguridad de Información  Todas las dependencias
	Elaborar un de Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y Estado de implementación .	1-03-2024	30-04-2024	Documento Plan de implementación de controles de seguridad y privacidad de la información	Oficina Asesora de Planeación  Oficial de seguridad de Información
	Identificar nuevos activos de información en cada dependencia en el Levantamiento Activos de Información con alcance a los procesos modificados en el 2024	30-09-2024	20-11-2024	Matriz actualizada SDI.PR.02.F.01 Identificación y clasificación de activos de información	Oficina Asesora de Planeación Oficial de seguridad de Información  Todos los procesos
	Envío del consolidado de activos de seguridad digital a la Secretaria General , para el respectivo reporte del índice de información clasificada y reservada y de Publicación de activos de la información JBB	25-11-2024	30-11-2024	Entrega de Matriz actualizada SDI.PR.02.F.01 Identificación y clasificación de activos de información	Oficina Asesora de Planeación  Secretaria General
	Recolectar bases de datos, bases de datos personales de acuerdo con los estándares emitidos por la Superintendencia de Industria y Comercio	30-01-2024	30-03-2024	Matriz de bases de datos personales de para reportar	Oficina Asesora de Planeación  Profesional de Datos personales
	Registrar y actualizar de las bases de datos Gestión de datos personales ante la Superintendencia de Industria y Comercio	01-04-2024	31-12-2024	Soporte de registro de actualización de las bases de datos personales de para reportar JBB	Oficina Asesora de Planeación  Profesional de Datos personales
	Definir una matriz que permita identificar los	30-01-2024	30-05-2024		Oficina Asesora de Planeación

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 18 de 21	



FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
	datos y el componente de la aplicación o el sistema de información en donde se dará su recolección y posterior almacenamiento.			Documento matriz de identificación de los datos y el componente de la aplicación o el sistema de información en donde se dará su recolección y posterior almacenamiento	Profesional de Datos personales
	Elaborar e incluir avisos de la privacidad que contenga el lenguaje mínimo señalado en la ley 1581 de 2012 y decreto 1377 de 2013.	30-01-2024	30-06-2024	Generar y entregar los Avisos de la privacidad de datos personales para los diferentes aplicativos, formularios y donde requiera a aceptación de tratamiento de datos	Oficina Asesora de Planeación  Profesional de Datos personales
	Actualizar el proceso de gestión de la tecnología en la seguridad de las comunicaciones	01-03-2024	30-07-2024	Documentar la gestión de Redes del JBB que incluya (Seguridad de redes, Seguridad de los servicios de red y Segregación de redes, adicionalmente las políticas de navegación de la Entidad)	Secretaria General - Sistemas
	Elaborar Documentación del proceso de gestión de la tecnología en la seguridad de eliminación de la Información	01-03-2024	30-07-2024	Documento Instructivo de borrado de la información sobre sistemas, aplicaciones y servicios, que no debe conservarse más tiempo del necesario para reducir el riesgo de divulgación no deseada	Secretaria General - Sistemas  Oficial de seguridad de Información

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muis</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				 <p>BOGOTÁ JARDÍN BOTÁNICO DE BOGOTÁ</p>
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 19 de 21	

FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
<b>EVALUACIÓN Y DESEMPEÑO SDI</b>	Seguimiento de indicadores de SDI	30-09-2024	31-12-2024	Reportar el monitoreo y seguimiento de indicadores de SDI en el aplicativo.	Oficina Asesora de Planeación Oficial de seguridad
	Elaborar reporte de ejecución y Seguimiento de Plan de implementación de controles de seguridad y privacidad de la información	30-09-2024	31-12-2024	Reporte de gestión de Plan de implementación de controles de seguridad y privacidad de la información – Seguridad Digital	Oficina Asesora de Planeación Oficial de seguridad
	Elaborar los informes de Seguimiento de riesgos de Seguridad de la Información – Seguridad Digital	30-04-2024	31-12-2024	Informe cuatrimestral de Riesgos de seguridad de la Información – Seguridad Digital	Oficina Asesora de Planeación Oficial de seguridad
	Elaborar reporte de gestión de incidentes de Seguridad de la Información – Seguridad Digital y Datos personales	30-09-2024	31-12-2024	Reporte de gestión de incidentes de Seguridad de la Información – Seguridad Digital y Datos personales 2024	Oficina Asesora de Planeación Oficial de seguridad
	Actualizar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos	30-09-2024	31-12-2024	Documento Reporte de matriz de control de controles.pdf	Oficina Asesora de Planeación Oficial de seguridad
	Evaluación de Plan de Continuidad de La Operación	30-09-2024	31-12-2024	Realizar Informe de cumplimiento del Plan de Continuidad del negocio	Secretaria General - Sistemas Oficina Asesora de Planeación
	Realizar las acciones del Plan de auditorías que evidencia la programación de las auditorías de seguridad y privacidad de la información, con seguimiento de Control Interno	01-03-2024	31-12-2024	Ejecución de Planes de mejora SDI programados	Oficina Asesora de Planeación Oficina de Control Interno
	Reporte de cumplimiento de	01-12-2024	31-12-2024	Documento de reporte de la	Oficina Asesora de Planeación

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Múts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 20 de 21	

FASE	ACTIVIDADES	FECHA INICIO	FECHA FIN	META	RESPONSABLE
	SDI.PLA.01 Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales			vigencia de cumplimiento de SDI.PLA.01 Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales	Oficial de seguridad
<b>MEJORAMIENTO CONTINUO SDI</b>	Medir el cumplimiento Plan de Seguridad y Privacidad de la Información – Seguridad Digital 2024	01-02-2024	31-12-2024	Talero de control y/o cronograma de cumplimiento con el avance Plan de Seguridad y Privacidad de la Información – Seguridad Digital 2024	Oficina Asesora de Planeación  Oficial de seguridad
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	01-02-2024	31-12-2024	Informe de cumplimiento de acciones preventivas y correctivas de los planes de mejora propuestos de seguridad de la información – Seguridad Digital	Oficina Asesora de Planeación  Oficial de seguridad  Oficina de Control Interno

Tabla 1 Plan SDI Cronograma

## 8.6. MEDICION

Se medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%.

*N° de Actividades Ejecutadas / N° de Actividades Programadas*



## 9. CONTROL DE CAMBIOS




FECHA	VERSIÓN	DESCRIPCIÓN
31-01-2024	1	Actualización del Plan por cambio de vigencia en el cumplimiento de Decreto 612 de 2018

## 10. AUTORIZACIONES:

<b>ELABORADO POR:</b>	<b>REVISADO POR:</b>	<b>APROBADO POR:</b>
-----------------------	----------------------	----------------------

Verificar su vigencia en el Listado Maestro de Documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Jardín Botánico José Celestino Muts</p>	<b>MANUAL DE PROCESOS Y PROCEDIMIENTOS</b>				
	<b>SDI- SEGURIDAD DE LA INFORMACION</b>				
	<b>Plan: Plan de Seguridad y Privacidad de la Información – Seguridad Digital</b>				
	<b>Código:</b> SDI.PLA.02	<b>Versión:</b> 1	<b>Fecha:</b> 31/01/2024	<b>Página:</b> 21 de 21	

Nombre(s): Catherine Suárez Rodríguez	Firma(s): 	Nombre(s): Genny Paola Ambrosio Villegas	Firma(s): 	Nombre(s): José Alberto Amaya González	Firma(s): 
Cargo(s): Contratista Especialista Oficial de Seguridad OAP		Cargo(s): Contratista - Profesional Apoyo – OAP Especialista Datos personales - OAP		Cargo(s): Jefe Oficina Asesora de Planeación	

Versión impresa no controlada, verificar su vigencia en el Listado Maestro de Documentos

Verificar su vigencia en el Listado Maestro de Documentos