



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

COORDINACIÓN SISTEMAS
OFICINA ASESORA DE PLANEACIÓN

CONTROL DE CAMBIOS

Versión	Fecha	Descripción
1.0	Enero 2023	Se elabora documento en su primera versión.

TABLA DE CONTENIDO

1. Objetivo	4
2. Alcance del Plan de Seguridad y Privacidad de la Información	4
3. Marco Normativo.....	4
4. Resumen Ejecutivo	5
5. Plan de Seguridad y Privacidad de la Información	6

1. Objetivo

Este plan tiene como objetivo determinar las acciones que se realizarán para proteger la información que el Jardín Botánico de Bogotá José Celestino Mutis utiliza para proteger y promover las estrategias del JBB, mediante la gestión del riesgo asociada a la misionalidad de la entidad.

2. Alcance del Plan de Seguridad y Privacidad de la Información

La implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información - SGSI se realizará en todos los procesos del Jardín Botánico de Bogotá José Celestino Mutis, de acuerdo con el ciclo de mejora continua PHVA; esto incluye, las actividades de formalización de los procesos, procedimientos y documentación correspondiente al SGSI a través de su integración con el Sistema de Gestión de Calidad – SGC. Dando cumplimiento de esta forma a los requisitos del Modelo Integrado de Planeación y Gestión.

3. Marco Normativo

- Ley 1581 de 2012 del Congreso de la República, "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 2609 de 2012 de la Presidencia de la República, "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
- Decreto 1377 de 2013 del Ministerio de Comercio, Industria y Turismo, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- Decreto 612 de 2018 de la Presidencia de la República, "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 886 de 2014 del Ministerio de Comercio, Industria y Turismo, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".
- Ley 1712 de 2014 del Congreso de la República, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- NTC-ISO/IEC 27001:2013, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos (ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements).
- Decreto 103 de 2015 de la Presidencia de la República, "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 1083 de 2015 del Departamento Administrativo de la Función Pública, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual 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".
- Decreto 2106 de 2019 del Departamento Administrativo de la Función Pública, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública", en el cual se 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.
- Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones – versión 4. 2021.
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.

4. Resumen Ejecutivo

La implementación de las adecuadas medidas de protección de la información estratégica de negocio y la preservación de la confidencialidad de ésta son requisitos esenciales para garantizar la confianza de clientes proveedores y funcionarios, factor indispensable para lograr los objetivos institucionales en entidades del sector que administra y protege la información del sector.

La adopción de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, es una decisión de carácter estratégico que permite no solo el cumplimiento de los requisitos de ley sino la optimización de los recursos humanos, tecnológicos y administrativos

necesarios para reducir los riesgos que afectan la información presente en el entorno tecnológico actual.

El presente documento se elabora dando cumplimiento al 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, entre los que menciona el plan de tratamiento de riesgos de seguridad de la información.

Considerando la importancia de cumplir los requisitos normativos en materia de protección de información y mitigar los impactos de sanciones derivadas de su incumplimiento, se incluye una serie de actividades que responden al ciclo Planear-Hacer-Verificar-Actuar (PHVA) para el sistema de gestión de seguridad de la información en miras a la certificación en la norma internacional ISO 27001:2013 y dando cumplimiento con lo establecido por MINTIC.

El plan de seguridad y privacidad de la información contempla todos los requisitos necesarios para garantizar a la entidad el fortalecimiento de su gestión institucional mediante la mejora de la confianza de todas las partes interesadas en la adecuada protección de la información.

5. Plan de Seguridad y Privacidad de la Información

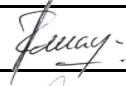
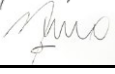
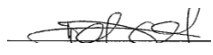
A continuación, se detallan las actividades a realizar durante el periodo del presente año 2023, se aclara que para su total cumplimiento la dirección debe garantizar los recursos en cuanto a personal, espacios y económicos para su implementación, conforme a los requerimientos legales y buenas prácticas de normas técnicas en todos sus procesos.

Dominio	Actividad	Responsable	Fecha estimada de Inicio	Fecha estimada de Finalización
Articulación MIPG – Gobierno Digital	Actualizar Instrumento de evaluación MSPI	Oficial de Seguridad	01/06/2023	30/11/2023
Planeación	Elaborar, formalizar y adoptar el manual de políticas del MSPI.	Oficial de Seguridad	15/02/2023	30/05/2023
Planeación	Realizar revisión y actualización periódica a la política general de Seguridad y Privacidad de la Información	Oficial de Seguridad	15/02/2023	30/05/2023
Planeación	Actualizar la declaración de aplicabilidad	Oficial de Seguridad	15/02/2023	30/11/2023
Activos de Información	Actualizar y modificar la matriz de inventario de activos de información	Oficial de Seguridad	15/02/2023	30/11/2023

Controles SDI	Socializar e implementar procedimiento TEC.PR.07.I.02 Autenticación de doble Factor y activar opción de seguridad de control de acceso de dispositivos no conocidos de Microsoft.	Oficial de Seguridad Profesional de Infraestructura	15/02/2023	30/11/2023
Controles SDI	Crear los procedimientos de Gestión de Dispositivos Móviles y Equipos Personales que acceden a Servicios de TI.	Oficial de Seguridad Profesional de Infraestructura	15/02/2023	30/11/2023
Controles SDI	Actualizar y/o complementar e implementar la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos: - Procedimiento TEC.PR.09	Oficial de Seguridad Profesional de Infraestructura	15/02/2023	30/11/2023
Controles SDI	Crear, actualizar y/o complementar e implementar la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos: - Política y Procedimiento de Gestión de Llaves Criptográficas	Oficial de Seguridad	15/02/2023	30/11/2023
Controles SDI	Crear, actualizar y/o complementar e implementar la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos: - Procedimiento de gestión de cambios en plataforma tecnológica	Oficial de Seguridad	15/02/2023	30/11/2023
Controles SDI	Crear, actualizar y/o complementar e implementar	Oficial de Seguridad	15/02/2023	30/11/2023

	<p>la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos:</p> <ul style="list-style-type: none"> - Procedimiento de gestión de ambientes. (Creación de procedimiento) 			
Controles SDI	<p>Actualizar y/o complementar e implementar la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos:</p> <ul style="list-style-type: none"> - Procedimiento de registro, monitoreo y medición de capacidad y desempeño 	Oficial de Seguridad	15/02/2023	30/11/2023
Requisitos Legales	<p>Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información</p>	Oficial de Seguridad	15/02/2023	30/11/2023
Gestión de Incidentes	<p>Actualizar y/o complementar e implementar la documentación del proceso de Gestión de la Tecnología y Seguridad de la Información considerando los siguientes elementos:</p> <ul style="list-style-type: none"> - Procedimiento de registro y seguimiento de eventos de sistemas de Información y comunicaciones 	Oficial de Seguridad	15/02/2023	30/11/2023
Gestión de Incidentes	<p>Actualizar y/o complementar e implementar el Procedimiento SDI.PR.01 Gestión de incidentes de Seguridad de la Información</p>	Oficial de Seguridad	15/02/2023	30/11/2023
Gestión de Incidentes	<p>Gestionar cada vez que se presente los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.</p>	Oficial de Seguridad	15/02/2023	30/11/2023
Gestión de Incidentes	<p>Socializar los boletines informativos de seguridad, Integrar con la Alta Consejería</p>	Oficial de Seguridad	15/02/2023	30/11/2023

	y de ser necesario con el CSIRT de Gobierno			
Vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Oficial de Seguridad	15/02/2023	30/11/2023
Indicadores SGSI	Formular, Implementar, actualizar y reportar los indicadores del SGSI	Oficial de Seguridad	15/02/2023	30/11/2023
Auditoría	Apoyar y acompañar las auditorías internas o externas que sean programadas en la Entidad.	Oficial de Seguridad	01/07/2023	30/11/2023
Gestión de Cambio y Apropriación	Desarrollar jornadas de sensibilización sobre la aplicación de los lineamientos de SDI	Oficial de Seguridad	15/03/2023	30/11/2023

	Nombre	Firma	Fecha
Aprobado por:	José Alberto Amaya González, Jefe Oficina Asesora de Planeación		(31/01/2023)
Revisado por:	Jorge Eliecer Lozano Ospina, Coordinador de Sistemas		(31/01/2023)
Elaborado por:	Diego Quiroga Sosa, OAP Oficina Sistemas		(31/01/2023)