PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA ASESORA DE PLANEACIÓN

2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.

JARDÍN BOTÁNICO DE BOGOTÁ

BOGOTÁ

CONTENIDO

1. INTRODUCCIÓN

El Jardín Botánico de Bogotá "José Celestino Mutis"-JBB, mediante Gestión de Riesgos de Seguridad de la Información realiza la identificación, análisis, valoración, evaluación y tratamiento, a fin de contribuir al cumplimiento de los requisitos de la entidad, propendiendo el cumplimiento de sus objetivos estratégicos, requisitos legales y reglamentarios, visión y misión, conservación de la confidencialidad, integridad y disponibilidad de la información.

En relación con lo anterior el Jardín Botánico de Bogotá estableció un manual Gestión de Riesgos de Seguridad de la Información donde, se articula con los lineamientos establecido en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" - Versión 5 de diciembre de 2020 publicada por el Departamento Administrativo de la Función Pública -DAFP, en el cual se establece el numeral "5. Lineamientos riesgos de seguridad de la información". a través de Anexo 4 Lineamientos para La Gestión de Riesgos de Seguridad Digital en Entidades Públicas, igualmente Identifica los riesgos de seguridad de la información de los procesos del Jardín Botánico de Bogotá, con el fin de mitigar los posibles efectos de su materialización el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos, Establece actividades de control para mitigar los riesgos de seguridad de la información asociados a los diferentes procesos, Monitorea los riesgos de seguridad de la información que se identifiquen y establezcan en la matriz de riesgos y Genera la cultura de la gestión del Riesgo de Seguridad y Privacidad de la Información.

En este sentido, la Entidad, mediante la definición del Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información, genera actividades y acciones preventivas para la mitigación de los riesgos, con el fin de mantener en su valoración un riesgo residual aceptable, a través de estrategias, identificación, análisis, tratamiento, evaluación y seguimiento, periódico de los riesgos de seguridad digital para cada uno de los procesos de la entidad identificados y promover una cultura de seguridad digital en relación a la importancia de dar un tratamiento adecuado a la información alineado contexto de los riesgos asociados que podrían comprometer el cumplimiento de los objetivos de la Entidad

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, 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 adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior del Jardín Botánico de Bogotá, aprobado por comité del Modelo Integrado de Gestión del 25 de enero de 2024.

2. OBJETIVO

Definir y aplicar acciones pertinentes que permitan identificar y tratar los Riesgos de Seguridad Digital y Privacidad de la Información por los responsables de los procesos de Entidad, así como gestionar los riesgos en materia de seguridad digital, identificados a partir del inventario de activos de información y valorados de acuerdo con el nivel de criticidad, protegiendo y preservando su confidencialidad, integridad y disponibilidad.

3. OBJETIVOS ESPECÍFICOS

- ✓ Identificar los riesgos de seguridad de la información asociados a los activos de seguridad digital críticos de los procesos del Jardín Botánico de Bogotá, con el fin de mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos.
- ✓ Gestionar los riesgos de seguridad. Digital mediante ejercicios de análisis, evaluación, valoración y seguimiento periódicos para preservar la integridad, disponibilidad y confidencialidad de los activos identificados por proceso.
- ✓ Fortalecer y apropiar cultura en los colaboradores referente a la gestión Riesgos de Seguridad Digital y Privacidad de la Información Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

4. ALCANCE

El presente documento se aplica para todos los procesos del Jardín Botánico de Bogotá (JBB), a los colaboradores de todos los niveles, desde la identificación de los riesgos de seguridad de la información que se encuentran en los niveles “Alto” y “Extremo” en la Matriz de riesgos de Seguridad de la Información de JBB hasta la definición del plan de tratamiento, responsables, fechas de implementación y seguimiento, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

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, Titulo 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.

Decreto 235 de 2010, por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

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 Libro2 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 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.

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.) 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).

- **Mapa de Riesgos**: Documento con la información resultante de la gestión del riesgo de seguridad de la información

- **Política de Administración de Riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo

- **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, 2021).

- **Plan de Tratamiento de Riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **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).

- **Riesgo de Imagen o Reputacional:** Posibilidad de ocurrencia de un evento que afecten la imagen, buen nombre o reputación del Jardín Botánico de Bogotá, ante sus clientes y partes interesadas.

- **Riesgos de Seguridad de la Información:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses del Jardín Botánico de Bogotá. Incluye aspectos relacionados con ambiente físico, digital y personas.

- **Riesgos Estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos del Jardín Botánico de Bogotá

- **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgos Operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales del Jardín Botánico de Bogotá.

- **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo de seguridad de la información.

- **Riesgos Tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad

- **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).

- **Tratamiento al Riesgo:** es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/CEI 27000, 2018).

7. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL

Jardín Botánico de Bogotá - JBB, deberá definir los roles y responsabilidades de las partes interesadas en lo concerniente a la gestión de riesgos, promoviendo el monitoreo y revisión a la gestión en sus etapas con el propósito de dar cumplimiento a los Mapas de Riesgos de Seguridad Digital y Privacidad de la Información proyectados, ejecutando los controles y acciones definidas, verificando la efectividad y el cumplimiento de los objetivos. Estas responsabilidades son acordes a la línea estratégica y las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG), donde se aprueban las directrices para la gestión del riesgo en la entidad y la revisión y/o mejora de las políticas establecidas.

En este sentido se establece una metodología de la cual se adelantan las actividades de gestión necesarias para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI articulándolo con el Modelo Integrado de Planeación y Gestión MIPG, por ello, los riesgos identificados que pueden afectar la disponibilidad, integridad y confidencialidad de la información y las acciones definidas contribuyen a la preservación de estos principios de seguridad de la información.

Ilustración 1 Metodología de Riesgos de seguridad SDI.PR.01.M.01

Para contemplar la metodología se define una línea metodológica así:

Ilustración 2 Línea metodológica Riesgos SDI

Las entidades públicas deben estructurar lineamientos que orienten la toma de decisiones para el manejo y tratamiento de los riesgos de Seguridad de la información identificados en los procesos, dando cumplimiento de la normatividad proferida para la implementación del Modelo Integrado de Planeación y Gestión en las entidades de estado, las disposiciones del Decreto 1499 de 2017 que modifica al Decreto 1083 de 2015, que actualiza el MECI incluyéndolo en el nuevo Modelo Integrado de Planeación y Gestión- MIPG, para lo cual se han determinado los siguientes: La Oficina Asesora de Planeación – Equipo de Sistemas, se determina como responsable en el desarrollo e implementación del SIG quien define la metodología para la administración del riesgo de acuerdo con los lineamientos otorgados por el DAFP, y que a su vez se ajusta a los procesos del Jardín Botánico de Bogotá. De igual manera genera las herramientas necesarias para identificación y valoración del riesgo en la entidad, sustentado en asesorías y acompañamiento constante.

Con el fin de controlar y mitigar los riesgos de seguridad de la información identificados, que permita promover una gestión preventiva, detectiva y correctiva; fomentando una cultura de autocontrol y empoderamiento liderado por la Alta dirección, los líderes de los procesos, responsables de área (directores, Jefes y coordinadores) para que sean garantes y participen en la aplicación de la administración del riesgo de seguridad de la información junto con sus equipos de trabajo.

7.2. LÍNEAS DE DEFENSA

Basados en el modelo de las tres líneas de defensa, el Modelo Estándar de Control Interno MECI y lo suministrado por la “Guía para la administración del riesgo y el diseño de controles en entidades

públicas - Versión 5 de diciembre de 2020" del Departamento Administrativo de la Función Pública DAFP, a continuación, se relacionan las responsabilidades de cada una de las instancias que participan en la gestión del riesgo.

LÍNEAS DE DEFENSA	ROL/ RESPOSABLE	ACTIVIDADES
Primera Línea de Defensa **1. Línea Estratégica** **2. Alta Dirección** 3. Comité Institucional de Coordinación de Control Interno CICCI	**Líderes de Procesos con el apoyo de los Enlaces designados por Procesos**	1) Da a conocer a su equipo de trabajo la política de administración del riesgo institucional. 2) Identifica y valora los riesgos que puedan afectar el logro de los objetivos institucionales y de los procesos. 3) Establece los controles idóneos que permitan administrar los riesgos identificados. 4) Realiza seguimiento permanente a los mapas de riesgos y reporta de acuerdo con la periodicidad establecida. 5) Hace modificaciones al mapa de riesgos del proceso cuando se requiera.
Segunda Línea de Defensa	**Oficina Asesora de Planeación**	1) Realiza asesoría y acompañamiento en la identificación de los riesgos y en la aplicación de la metodología establecida. 2) Realiza seguimiento a la administración de riesgos ejecutada por los procesos, asegurando que los resultados sean los esperados, de no ser así, deben pronunciarse y asesorar a los procesos en los cambios a los que haya lugar. 3) Consolida los seguimientos a los mapas de riesgos.
	Servidores Públicos – delegados grupo operativo	1) Informa sobre la materialización de los riesgos, la identificación de nuevos riesgos potenciales y evalúan si la valoración del riesgo es la apropiada. 2) Adelanta seguimiento a los mapas de riesgos. 3) Socializa al interior de los procesos los mapas de riesgos.
Tercera Línea de Defensa	**Oficina de Control Interno**	1) La Oficina de Control Interno alerta situaciones que generen un posible riesgo (corrupción, gestión, seguridad de la información) en el desarrollo de las actividades ejecutadas por los procesos de la entidad, como resultado de las auditorías internas. 2) Se encarga comunicar al CICCI posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. 3) Se encarga de revisar la efectividad y la aplicación de controles establecidos en los mapas de riesgos.
Responsabilidad de Seguridad Digital	**Oficial de seguridad**	Además de las líneas de defensa mencionadas y de acuerdo con lo establecido por el Ministerio de Tecnologías de la información y las comunicaciones, el Jardín Botánico de Bogotá - JBB delega la responsabilidad de gestionar los riesgos de seguridad de la información, al encargado de seguridad de la información, quien apoya en la identificación de los activos de información, su clasificación e identificación de infraestructuras criticas cibernéticas, establecimiento de controles para evitar la pérdida de confidencialidad, integridad y/o disponibilidad de la información de la entidad. El oficial de seguridad de la información es el encargado de realizar el

LÍNEAS DE DEFENSA	ROL/ RESPOSABLE	ACTIVIDADES
	Profesional Datos personales	análisis de riesgos anualmente, realizar el seguimiento y cada vez que se presente un cambio representativo en los activos tecnológicos o informáticos debe actualizar la información respectiva. El profesional de datos personales es el encargado de efectuar el análisis de riesgos correspondientes la protección de los datos personales recolectados por la entidad para mitigación los riesgos del Tratamiento de Datos personales

7.3. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN (RIESGOS DE SEGURIDAD DIGITAL)

La gestión de los Riesgos de Seguridad Digital y Privacidad de la Información se ejerce en integración con el MSPI (Modelo de Seguridad y Privacidad de la Información) y con el MGRSD (Modelo de Gestión de Riesgos de seguridad de la información) determinado por MINTIC. Así mismo, en la determinación de las fases para la gestión de riesgos, se incluyen las ICC (Infraestructuras Críticas Cibernéticas) como parte de los activos de la información del Jardín Botánico de Bogotá.
Por lo anteriormente mencionado se definieron etapas para la gestión de Riesgos de Seguridad Digital y Privacidad de la Información en la entidad con el desarrollo del ***SDI.PR.01.M.01 Manual Gestión de Riesgos de Seguridad de la Información*** así:

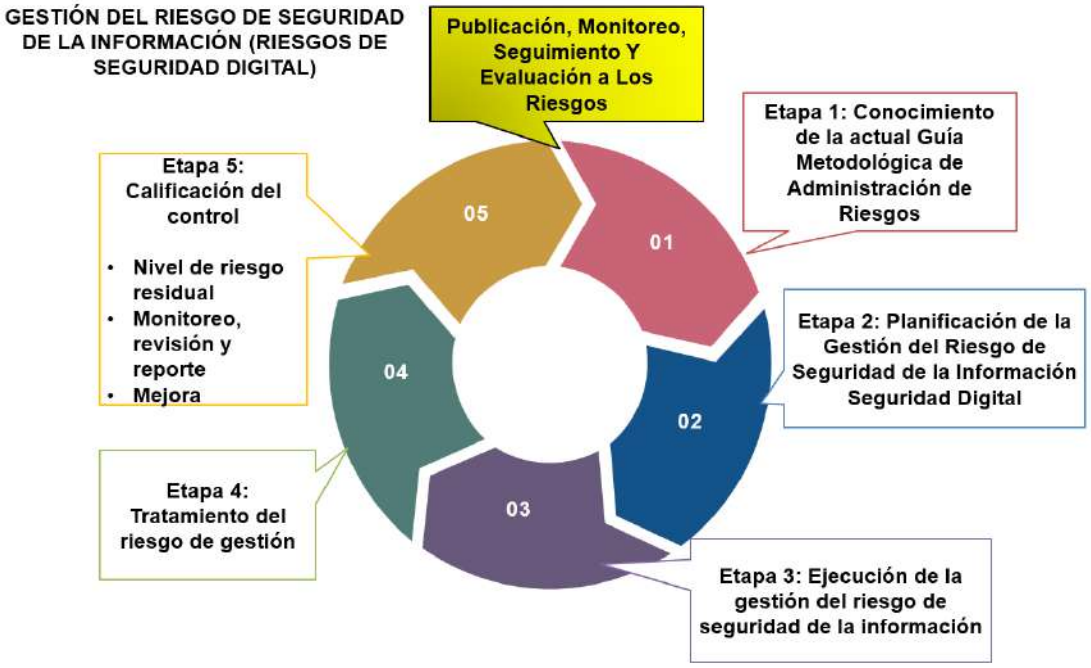

Ilustración 3 desarrollo del SDI.PR.01.M.01 Manual Gestión de Riesgos de Seguridad de la Información

7.4. PLAN DE TRABAJO

El Plan de implementación de Riesgos de Seguridad Digital y Privacidad de la Información, para la aplicación del habilitador de seguridad de la información de la Política de Gobierno Digital[1], 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 (PAI).

Fase	Acciones	Fecha de inicio	Fecha Fin	Meta/ Producto	Responsable
Planeación	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 Digital y Privacidad de la Información 2024	Oficina Asesora de Planeación Oficial de seguridad de Información
Sensibilización	Socialización de lineamientos, documentos y/o Herramienta Gestión de Riesgos de Seguridad Digital y Privacidad de la Información	15-02-2024	15-03-2024	Formato listado de asistencia y/o asistencia por Teams Acta y/o grabación	Oficina Asesora de Planeación Oficial de seguridad de Información
Identificación, análisis, valoración de Riesgos de Seguridad Digital y Privacidad de la Información	Realizar acompañamiento en la Identificación, Análisis, valoración de controles y definición del manejo de los Riesgos de Seguridad Digital y Privacidad de la Información a los procesos con riesgos asociados	15-02-2024	15-03-2024	Acta de mesa de trabajo Documento Matriz de Riesgos de Seguridad de la Información.	Oficina Asesora de Planeación Oficial de seguridad de Información Líderes de Procesos JBB
	Realizar la realimentación, revisión verificación y aprobación de Riesgos de Seguridad Digital y Privacidad de la Información identificados con sus planes de tratamiento y controles existentes de los procesos.	18-03-2024	30-03-2024	Correo Electrónico Documento actualizado Matriz de Riesgos de Seguridad de la Información	Líderes de Procesos JBB

[1] https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Fase	Acciones	Fecha de inicio	Fecha Fin	Meta/ Producto	Responsable
Seguimiento, evaluación y monitoreo de los riesgos	Establecer las fechas y avances para el seguimiento de los planes de tratamiento y controles existente por parte del Líder del Proceso	18-03-2024	30-03-2024	Acta de mesa de trabajo Documento Matriz de Riesgos de Seguridad de la Información.	Líderes de Procesos JBB Oficial de seguridad de Información
	Realizar seguimiento a los Riesgos de Seguridad Digital y Privacidad de la Información identificados asociados a los procesos en el mapa de riesgo con sus planes de tratamiento, evaluación de riesgos residuales y controles existentes con las evidencias correspondientes. Cuatrimestralmente	01-04-2024	30-12-2024	Matriz actualizada SDI.PR.02.F.01 Identificación y clasificación de activos de información Carpeta de Evidencias de aplicación del control	Oficina Asesora de Planeación Oficial de seguridad de Información Líderes de Procesos JBB
Monitoreo, Revisión y mejora	Monitorear y reportar el resultado de las actividades actividad de control, que se aplicaron necesarias con el fin de minimizar o mitigar el riesgo y de este modo evitar los daños intrínsecos del factor del riesgo, definidas en los planes de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información por proceso e JBB, así como las oportunidades de mejora .	01-04-2024	30-12-2024	Informe cuatrimestral de Riesgos de Seguridad Digital y Privacidad de la Información	Oficina Asesora de Planeación Oficial de seguridad

Ilustración 4 Cronograma de Pla de Riesgos SDI

7.5. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información identificados en la Entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

7.6. MEDICION

Se medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%, de las actividades definidas en el plan de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información que está orientado principalmente a determinar el porcentaje de ejecución de actividades definidas.

N° de Actividades Ejecutadas /N° de Actividades Programadas

8. 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

9. AUTORIZACIONES:

ELABORADO POR:		REVISADO POR:		APROBADO POR:	
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	