PLAN DE TRATAMIENTO DE RIEGSOS 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

Introducción

La seguridad y privacidad de la información en las entidades tiene como objetivo la protección de cualquier tipo de activo de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad y privacidad de la información, que permitan gestionar y reducir los riesgos e impactos a los cuales está expuesta la entidad y se logre alcanzar el máximo retorno de inversión con relación al cumplimiento de la misión y visión institucionales.

1. Objetivo

Gestionar los riesgos de seguridad de la información digital a través del presente plan, el cual proporciona las pautas necesarias para realizar el análisis, valoración, seguimiento y monitoreo permanente de los riesgos encaminados al cumplimiento y mejoramiento continuo, de tal forma que se definan y apliquen los controles de seguridad con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información digital en la entidad.

2. 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.

3. Términos y Definiciones

- Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la entidad.

- Administración del riesgo: comprende el conjunto de elementos de control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera negativa el logro de sus objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- Amenaza: es la causa potencial de una situación de incidente y no deseada por la organización.

- Análisis de riesgos: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo.

- Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- Estimación del riesgo: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- Evaluación de riesgos: combinación de la probabilidad de ocurrencia de un riesgo con el impacto de su materialización, que permite determinar el grado de exposición de la entidad.

- Evento: un incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo específico. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

- Impacto: las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Integridad: propiedad de la información relativa a su exactitud y completitud.

- Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- Riesgo inherente: es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- Riesgo residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.

- Vulnerabilidad: es aquella debilidad de un activo o grupo de activos de información, o de un control que puede ser explotada por una o más amenazas.

4. Tratamiento del Riesgo

La conservación de la seguridad de la información requiere de mayor detalle frente a los constantes avances tecnológicos, en cuanto a la masificación de la información y las comunicaciones. Lo cual conlleva a que se presenten Riesgos de Seguridad de la Información, que deben ser identificados y gestionados. Para ello, este documento técnico permite establecer y adoptar mecanismos integrales a todos los procesos contribuyendo a la reducción o mitigación de los riesgos de seguridad digital, contemplados desde el Modelo de Seguridad y Privacidad de la Información del MinTIC a los que la entidad puede estar expuesta respecto a los activos de la información.

Por ende, para la consecución del cumplimiento de los objetivos estratégicos y la misionalidad del Jardín Botánico de Bogotá (en adelante JBB), estos riesgos forman parte del marco de la confidencialidad de los activos de información, bajo el enfoque de la gestión del riesgo de la seguridad de la Información, como componente esencial del gobierno corporativo, sustentado en integridad, ética y disponibilidad de la información misma. Por tal razón, se hace necesaria la implementación de una Guía Metodológica de la Gestión de los Riesgos de Seguridad de la Información, en el cual se establece la ruta estratégica para la planificación y desarrollo del SGSI "Subsistema de Gestión de Seguridad de la Información" aplicando un plan de tratamiento de los riesgos, apoyado en documentos y herramientas que permitan proteger y conservar los Sistemas de Información, así como la Información e infraestructura tecnológica de la entidad.

El documento técnico "Manual Gestión de Riesgos de Seguridad de la Información" establece los lineamientos para la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misionalidad y el cumplimiento de los objetivos estratégicos, la gestión de los procesos, proyectos y planes del Jardín Botánico de Bogotá asociados a los Riesgos de Seguridad información.

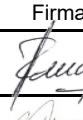
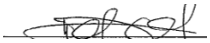
Para ello mediante el acta 32-2022 de revisión, modificación, aprobación y adopción de documentos asociados al SIG fue aprobada la creación del "Manual Gestión de Riesgos de Seguridad de la Información" la cual enmarca la gestión desde las tres líneas de defensa en donde participan todos los colaboradores del Jardín Botánico de Bogotá, independientemente de su forma de vinculación incluyendo servidores públicos, contratistas y subcontratistas en el desarrollo de sus funciones y compromisos.

5. Plan de Tratamiento de Riesgos de Seguridad de la Información

Conforme a los riegos de identificados los siguientes son los controles establecidos para el tratamiento de estos:

RIESGO	Descripción de la Acción, basado en el análisis de causas	Responsable (Cargo)	Fecha de Inicio	Fecha de Finalización
Por ataques cibernéticos debido a la ejecución de código malicioso, malware, ransomware o cualquiera de sus derivadas.	1. realizar el estudio y gestión para que las cuentas de usuario del LDAP (cuentas de red de usuario) estén sincronizadas con el sistema de información Central de cuenta. 2. usar factores de doble autenticación en el sistema de información Central de cuentas.	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de Redes y técnico de apoyo y soporte	1 de abril de 2023	31 de diciembre de 2023
Por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones.	1. realizar el estudio y gestión para que las cuentas de usuario del LDAP (cuentas de red de usuario) estén sincronizadas con el sistema de información Central de cuenta. 2. usar factores de doble autenticación en el sistema de información Central de cuentas.	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de Redes y técnico de apoyo y soporte	1 de abril de 2023	31 de diciembre de 2023
Por uso indebido de privilegios y/o fallas de operación de los controles técnicos establecidos debido al no monitoreo de los controles establecidos	1. realizar el estudio y gestión para que las cuentas de usuario del LDAP (cuentas de red de usuario) estén sincronizadas con el sistema de información Central de cuenta. 2. usar factores de doble autenticación en el sistema de información Central de cuentas.	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de Redes y técnico de apoyo y soporte	1 de abril de 2023	31 de diciembre de 2023
Por modificación indebida de los registros ingresados debido al acceso no autoriza al aplicativo y la base de datos que contiene los registros	1. realizar el estudio y gestión para que las cuentas de usuario del LDAP (cuentas de red de usuario) estén sincronizadas con el sistema de información Central de cuenta. 2. usar factores de doble autenticación en el sistema de información Central de cuentas.	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de Redes y técnico de apoyo y soporte	1 de abril de 2023	31 de diciembre de 2023
Por indisponibilidad o perdida de la integridad de los datos debido a la modificación de los registros almacenados o daños para lectura	1. realizar el estudio y gestión para que las cuentas de usuario del LDAP (cuentas de red de usuario) estén sincronizadas con el sistema de información Central de cuenta. 2. usar factores de doble autenticación en el sistema de información Central de cuentas. 3, Validar controles criptográficos para asegurar la validez del documento	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de redes y telecomunicaciones Administrador del sistema de información	1 de abril de 2023	31 de diciembre de 2023

Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos	Validar la ampliación del recurso humano para distribuir tareas y asignar responsabilidades, Generar espacios físicos seguros donde tenga solo acceso el propietario de la información Remitir solicitudes por correo electrónico certificado Validar backups periódicos en la nube usar factores de doble autenticación para acceso a la cuenta de servicio en Office 365	Propietario del activo de información Equipo de trabajo Oficial de Seguridad de la Información Profesional de Redes y técnico de apoyo y soporte	01 de abril de 2023	31 de diciembre de 2023
Por modificación indebida de los registros ingresados debido al acceso no autorizado al aplicativo y la base de datos que contiene los registros	1, Validación con los interventores o supervisores de contrato de cuales usuarios van a ingresar al sistema de información, que actividades realizaran en la plataforma y así mismo asignarlos los permisos necesarios dentro de la aplicación	Administrador del sistema de información de cada modulo	1 de abril de 2023	31 de diciembre de 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)