JARDÍN BOTÁNICO JOSÉ CELESTINO MUTIS

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSION DEL DOCUMENTO:
01

TABLA DE CONTENIDO

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
12/09/2019	1	Se ajusta y adopta la Política General de Seguridad.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL JARDÍN BOTÁNICO JOSÉ CELESTINO MUTIS

1. INTRODUCCIÓN

La 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 Subsistema de Gestión de Seguridad de la Información, 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.

El Subsistema de Gestión de Seguridad de la Información (SGSI) hace parte del Sistema Integrado de Gestión del Jardín Botánico José Celestino Mutis. Este subsistema contiene las políticas técnicas, procedimientos, directrices, metodologías y controles necesarios para la efectiva gestión de la seguridad de la información, alineados con lo estipulado por la política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión, el Modelo de Seguridad y Privacidad de la Información y la norma ISO 27001:2013 como referencia.

2. OBJETIVO

Establecer las condiciones de uso confiable de la información el entorno digital y físico, realizando una adecuada gestión de los riesgos, preservando la confidencialidad, integridad y disponibilidad de la información tratada, y de los servicios que se prestan al ciudadano.

3. OBJETIVOS ESPECÍFICOS

- Garantizar la gestión adecuada de la seguridad de la información tratada en los servicios prestados al ciudadano, la investigación, el mejoramiento de la calidad ambiental y la educación ambiental.
- Establecer los lineamientos de seguridad de la información necesarios que apoyen la gestión efectiva y transparente que ayuden a incrementar la importancia, credibilidad y confianza en el Jardín Botánico José Celestino Mutis.
- Proteger la información, promoviendo siempre la aplicación de las mejores prácticas de seguridad de la información de manera responsable, teniendo en cuenta el valor implícito que tienen los recursos financieros, humanos, físicos y ambientales utilizados en el Jardín Botánico José Celestino Mutis.
- Establecer una cultura entre los funcionarios, terceros, aprendices, practicantes y grupos de interés del Jardín Botánico José Celestino Mutis del tratamiento seguro de la información.

- Gestionar oportuna y adecuadamente los riesgos de seguridad de la información Jardín Botánico José Celestino Mutis.

4. ALCANCE

La Política General de Seguridad y Privacidad de la Información aplicará a todos los procesos, procedimientos, y tratamientos de información que realice el Jardín Botánico José Celestino Mutis, a terceros que traten información en nombre del Jardín Botánico José Celestino Mutis o a quienes se transfiera o trasmita información cuyo responsable sea el Jardín Botánico José Celestino Mutis.

Para los efectos relacionados, la política aplicará a las dependencias del Jardín Botánico de acuerdo con la estructura orgánica-funcional vigente, establecida en los Acuerdos 11 de 2001 y 02 de 2007 : Dirección, Secretaría General y Control Disciplinario, Oficina Asesora Jurídica, Oficina de Control Interno, Subdirección Científica, Subdirección Técnica Operativa, Subdirección Educativa y Cultural y Oficina de Arborización; así también al director(a), subdirectores, jefes de oficina, servidores de carrera administrativa y de libre nombramiento y remoción y contratistas.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Jardín Botánico José Celestino Mutis reconoce la seguridad de la información requerida en los procesos de investigación, gestión, educación y administrativos preservando la confidencialidad, integridad y disponibilidad de la información, realizando una adecuada gestión de los riesgos de seguridad de la información, implementando los controles necesarios que permitan mitigar los riesgos, sensibilizando, educando y comprometiendo a su recurso humano en el manejo seguro de la información, cumpliendo los requisitos legales, las necesidades de la entidad y de las partes interesadas en seguridad de la información.

6. TÉRMINOS Y DEFINICIONES

Las definiciones de la Política General de Seguridad y Privacidad de la Información del Jardín Botánico José Celestino Mutis, tiene fundamento en el estándar internacional ISO 27000.

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: Posible causa de un incidente no deseado, que puede producir daño a un sistema u organización.

Análisis de riesgos: Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo.

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

Control: Medida que modifica el riesgo. Sinónimo salvaguarda.

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

Gestión de riesgos: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

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.

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.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Tercero: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.

7. MARCO NORMATIVO

Ley 527 de 1999 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos: El mensaje de datos es "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax".

Ley 594 de 2000 Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones: Responsabilidad "Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos".
Administración y acceso. "Es una obligación del Estado la administración de los archivos públicos y un derecho de los ciudadanos el acceso a los mismos, salvo las excepciones que establezca la ley;"

Ley 599 DE 2000 Por la cual se expide el Código Penal: En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

Ley 734 de 2002 Por la cual se expide el Código Disciplinario Único: Art 34. Deberes. Son deberes de todo servidor público "4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos. "

La Ley 850 de 2003 Por medio de la cual se reglamentan las veedurías ciudadanas: Principio de Transparencia "A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia".

Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos: Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

Ley 1150 de 2007 Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos: Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.

Ley 1266 de 2008 Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países: Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

Ley 1221 de 2008 Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones: Teletrabajo. Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

Ley 1273 de 2009 Por medio de la cual 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: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones: Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.

Ley 1581 de 2012 Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales: Se hace referencia, principalmente, al artículo 15 de la Constitución Nacional en el cual se establece que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…".

Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones: El empleador debe informar al tele trabajador sobre las restricciones de uso de equipos y programas informáticos, la legislación vigente en materia de protección de datos personales, propiedad intelectual, seguridad de la información y en general las sanciones que puede acarrear por su incumplimiento.

Decreto 886 de 2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos: Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012".

Decreto Nacional 2573 de 2014 Estrategia de Gobierno en Línea de la República de Colombia: E, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad

Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública: Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley".

Decreto 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones: "La información pública que contiene datos semiprivados o privados, definidos en los literales g) y h) del artículo 3° de la Ley 1266 de 2008, o datos personales o sensibles, según lo previsto en los artículos 3° y 5° de la Ley 1581 de 2012 y en el numeral 3° del artículo 3° del Decreto 1377 de 2013, solo podrá divulgarse según las reglas establecidas en dichas normas."

CONPES 3701 Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país: Este documento define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas, fortalecer las capacidades

del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

CONPES 3854 por el cual se crea y justifica la Política Nacional de Seguridad Digital: El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.

Decreto 1499 del 11 de septiembre de 2017 Integración del Sistema de Gestión de Calidad y lo Sistemas de desarrollo administrativo: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Decreto 25 de agosto de 2017 Los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos: Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones.

8. RESPONSABILIDADES

Comité institucional de Gestión y Desempeño:

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de gobierno digital, seguridad digital y de la información. Establecido en el Capítulo II Funciones, Roles y Responsabilidades, Artículo Sexto, numeral 6 de la resolución número 411 de 2018.

Oficial de Seguridad de la Información:

- Diseñar, actualizar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a

decisión del Comité de Seguridad, realizando la implementación y seguimiento de los mismos.
- Coordinar la gestión de riegos de seguridad de la información de acuerdo con la periodicidad establecida, incluye la actualización de amenazas, vulnerabilidades y riesgos en los activos críticos e información sensible.
- Vigilar el seguimiento a las no conformidades, el estado de las acciones correctivas, además de las quejas reclamos y sugerencias sobre la seguridad de la información.
- Asegurar que se establecen, mantienen e implementan los procesos necesarios para el desarrollo del Sistema de Gestión de Seguridad de la Información.
- Presentar los informes de seguridad digital, incluyendo las principales novedades, iniciativas e incidentes de seguridad de la información, así como las lecciones aprendidas.
- Organizar las reuniones del comité de seguridad digital y/o convocar a comité extraordinario cuando las circunstancias o uno de sus miembros lo requieran, con motivo de riesgo mayor para la institución.
- Informar a la Alta Dirección sobre el desempeño del sistema de gestión de seguridad de la información y de cualquier necesidad de mejora.
- Estar en contacto con grupos especiales en temas de seguridad digital, con el fin de estar documentado acerca de los nuevos métodos y herramientas de ataque.
- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad digital.
- Realizar el proceso de gestión de incidentes de seguridad que se presenten en la entidad.
- Soportar a los líderes de proceso en el análisis de riesgos de seguridad de la información y consolidar los planes de manejo de los mismos.
- Elaborar las campañas de sensibilización, capacitación y socialización del Subsistema de Seguridad de la Información.

Coordinador de la Oficina de Sistemas

- Coordinar la administración y configuración de los recursos informáticos dentro de la plataforma tecnológica de seguridad.
- Planear y ejecutar el plan de mantenimiento y actualización de la infraestructura tecnológica y de telecomunicaciones de la entidad.
- Implementar las mejorar identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.
- Identificar y reportar riesgos, eventos o incidentes de ciberseguridad a través de los canales definidos.

Oficina de Control Interno

- Evaluar de manera independiente la eficiencia y los controles existentes con relación al funcionamiento de Subsistema de Seguridad de la Información,

verificando que estos permitan minimizar los riesgos y fortalecer la seguridad de la información en la entidad.

Secretaria General y de Control Disciplinario:

- Realizar los procesos disciplinarios por el incumplimiento de la política general de seguridad y privacidad, políticas técnicas y controles.

Gestión Humana

- Realizar la verificación de antecedentes de los funcionarios.
- Suscribir los acuerdos de Confidencialidad con los funcionarios.
- Coordinar con el Oficial de Seguridad el plan de inducción, capacitación y sensibilización en seguridad de la información.

Responsable de seguridad física

- Diseñar e implementar los controles para proteger el perímetro de seguridad física del Jardín Botánico José Celestino Mutis.
- Implementar y verificar los controles para el ingreso de las áreas seguras.
- Monitorear el sistema de video vigilancia.
- Reportar al Oficial de Seguridad de la Información cualquier incidente referente a las áreas seguras.

Líderes de proceso:

- Identificar y evaluar los activos de información a su cargo.
- Realizar el análisis de riesgos de seguridad de la información de sus procesos y coordinar el plan de tratamiento con el Oficial de Seguridad de la Información.
- Verificar los informes de auditorías realizadas a la seguridad digital y velar porque se apliquen las acciones correctivas identificadas, así como las recomendaciones entregadas por los auditores.

Funcionarios, contratistas y terceros:

- Cumplir las políticas, procedimientos y controles establecidos en el Subsistema de Gestión de Seguridad de la Información.
- Informar sobre cualquier incidente de seguridad de la información por los canales establecidos.
- Asistir a las sensibilizaciones en temas de Seguridad de la Información.

9. MANEJO DE DESVIACIONES Y EXCEPCIONES

Las desviaciones presentadas por el Subsistema de Gestión de Seguridad de la Información serán manejadas de acuerdo con la Política y el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

Las excepciones a las políticas, procedimientos y controles del Subsistema de Gestión de Seguridad deben ser evaluadas por el Oficial de Seguridad de la Información, teniendo en cuenta:

- El evento que genera la excepción.
- Los posibles riesgos que puedan presentarse con la excepción.
- El posible impacto que pueda generar a excepción.
- Las acciones para el manejo de la excepción.

Las excepciones según su nivel deben tener el visto bueno del líder de proceso y la evaluación y autorización del Oficial de Seguridad de la Información y/o el comité Comité institucional de Gestión y Desempeño.

10. FECHA DE ENTRADA EN VIGENCIA DE LA POLITICA

La presente política es adoptada por medio de la resolución 413 del 12 de Septiembre de 2019 y rige a partir de esta fecha.