PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

1 Objetivo

Este plan tiene como objetivo determinar las acciones que se realizaran 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

La implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información - SGSI en su tercera fase, 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 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.

MINTIC

ISO 217001:2013

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.

4 Actividades para desarrollar en la vigencia de 2022

A continuación, se detallan las actividades a realizar durante el periodo del presente año 2022, 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.

Gestión	Actividades	Tareas	Responsablede la Tarea	Fechas ProgramaciónTareas	
				Fecha Inicio	Fecha Final
Activos de Información	Socialización y sensibilización a todas las áreas y procesos sobre los lineamientos para mantener actualizado o identificar activos de información	Sesiones de trabajo por área y proceso durante el año	Responsables de las áreas y su equipo de trabajo Oficial de	Febrero-15-2022	Nov-30-2022

Gestión	Actividades	Tareas	Responsablede la Tarea	Fechas ProgramaciónTareas	
				Fecha Inicio	Fecha Final
			seguridad de la Información		
	Levantamiento y/o actualización de los Activos de Información	Socializar la metodología de activos de Información.	Oficial de seguridad de la Información	Febrero-15-2022	Nov-30-2022
		Validar activos de información en el instrumento levantado en la vigencia anterior	Enlace de cada proceso, Oficial de seguridad de la Información	Febrero-15-2022	Nov-30-2022
		Identificar nuevos activos de información en cada área	Enlace de cada proceso, Oficial de seguridad de la Información	Febrero-15-2022	Nov-30-2022
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Oficial de seguridad de la Información	Febrero-15-2022	Nov-30-2022
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	Febrero-15-2022	Nov-30-2022
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Enlaces de cada proceso	Febrero-15-2022	Nov-30-2022
	Publicación de Activos de Información	Validar y aceptar los activos de información parasu publicación en SIMIG por cada líder de proceso.	Enlace de cada proceso, Oficial de seguridad de la Información	Febrero-15-2022	Nov-30-2022
		Consolidar el instrumento de activos de Información.	Equipo de Activos	Nov - 1 de 2022	Dic-30-2022

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión deRiesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de Gestión de Riesgos	Ene-22-2022	Feb-14-2022
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Publicación	Publicación y socialización interna de la Matriz de riesgos	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Definición Seguimiento Fase deTratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Mejoramiento	Identificación de oportunidades de mejora acordea los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	Febrero-15-2022	Nov-30-2022

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado deincidentes de seguridad de lainformación	Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035.	Responsables de área y Oficial de seguridad de la Información la Información.	mar-15-2022	may-15-2022
		Socializar el procedimiento a los especialistas de la Oficina de sistemas, indicando los cambios en el procedimiento si los hubo.	Responsables de área y Oficial de seguridad de la Información la Información.	mar-19-2022	mar-26-2022
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento si los hubo	Responsables de área y Oficial de seguridad de la Información la Información.	mar-19-2022	mar-26-2022
		Socializar el procedimiento a los colabores de la Entidad.	Oficial de Seguridad de la Información	mar-19-2022	mar-26-2022
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar cada vez que se presente los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Especialistas Sistemas - Oficial de Seguridad de la Información	ene-18-2022	dic-31-2022
	Alta Consejería y CSIRT	Socializar los boletines informativos de seguridad, Integrar con la Alta Consejería y de ser necesario con el CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática	ene-22-2021	dic-15-2021
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Profesional de sistemas, Oficial de Seguridad de la Información.	ene-22-2021	dic-15-2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	ene-18-2022	feb-25-2022
	Publicar el plan	Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los enlaces de procesos	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	Feb-25-2022	mar-15-2022
	Ejecutar el Plan de Cambio yCultura de Seguridad y Privacidad de la Información,Seguridad Digital	Implementar las estrategias del Plan de Gestiónde Cultura Organizacional en Apropiación del SGSI	Enlace de procesos	mar-16-2022	dic-20-2022
	Analizar el Plan de Cambio yCultura de Seguridad y Privacidad de la Información,Seguridad Digital	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiacióndel SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	mar-16-2022	dic-20-2022
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de laInformación	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	ene-22-2022	dic-22-2022
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de laInformación	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	jun-21-2022	dic-21-2022
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Oficial de Seguridad de la Información	mar-3-2022	mar-31-2022
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	jun-4-2022	dic-21-2022
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad de la Información	may-15-2022	jun-14-2022

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	jun-15-2022	jul-14-2022
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información	abr-15-2022	dic-14-2022
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidadde la información	Oficial de Seguridad de la Información	abr-15-2022 oct -15 -2022	may-14-2021 Nov – 14-2022
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno, cuando aplique	Oficial de Seguridad de la Información	mar-1-2022	dic-20-2022
Auditorías Internas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas por control Interno	Todos los procesos	De acuerdo con programa dela OCI	De acuerdocon programa de la OCI
Indicadores SGSI	Provisión de información a los indicadores de mediciónde l SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad de la Información	ene-20-2022	dic-21-2022
		Reportar indicadores	Enlaces de procesos	ene-20-2022	dic-21-2022
Seguimiento a pruebas de Vulnerabilidad realizadas en la vigencia anterior	Iniciar seguimiento a la ejecución del plande remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis realizado la vigencia anterior	Oficial de Seguridad, OTI	Abr-1-2022	jun-30-2022
	Definir lineamientos para ejecutar análisis GAP, análisis de un retest de las vulnerabilidades encontradas en la vigencia anterior	Definir los lineamientos para la ejecución del RETEST, anexo técnico y el alcance para la realización de análisis GAP.	Oficial de Seguridad,OTI	jul-5-2022	Sep-30-2022
	Ejecutar el RETEST	Ejecución del RETEST , teniendo en cuenta los lineamientos definidos con la oficina de sistemas	Oficial de Seguridad, OTI	Ago-9-2022	nov-30-2021
	Iniciar la ejecución del plande remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis GAP, análisis de vulnerabilidades	Oficial de Seguridad, OTI	dic-1-2021	dic-31-2021
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficina Asesora Jurídica, Oficial de Seguridad y Secretaría General	feb-18-2022	jun-29-2022

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Revisión de bases de datos	Revisar y realimentar la información recolectadapor las áreas para el registro de las bases de datos	Oficial De Seguridad y Enlace de procesos	feb-1-2022	dic-20-2022
	Registro y actualización delas bases de datos	Registrar o actualizar las bases de datos teniendoen cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad	jul-22-2022	dic-20-2022

Las anteriores actividades se plantean realizar con cada uno de los procesos y áreas del JBB, con el fin de socializar con todos los procesos el Sistema de Gestión de Seguridad de la Información y generar conciencia de las responsabilidades que cada colaborador tiene frente a la protección de la información.

5 Condiciones generales para la ejecución del presente plan.

5.1 Medios y herramientas profesionales

De acuerdo con el requerimiento, las características del trabajo a realizar, las labores tendrán lugar en el nivel central, los desplazamientos a las demás territoriales, se realizarán según sea necesario o se podrán utilizar medios de conexión remota o a través de video conferencia.

Se utilizarán las herramientas profesionales requeridas para llevar a cabo las asignaciones, como por ejemplo computadora y programas de software (software de gerencia del proyecto, procesador de palabras, hoja electrónica, cliente de correo electrónico, navegador web,) teléfono celular y elementos de oficina.

5.2 Requerimiento de personal

De acuerdo con lo anteriormente descrito se requieren de al menos un profesional especialista en seguridad de la información y con la experiencia requerida para la implementación del sistema en entidades del estado colombiano.

Además de lo anterior se requiere que esta(s) persona(s) de respuesta y haga seguimiento a los eventos de seguridad, incidentes y de ser necesario a la ejecución de posibles contingencias. Así como seguimiento a los planes de acción fruto de las auditorías internas.