PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

TC-PL-03

Oficina de Tecnologías de la Información y las Comunicaciones

12/01/2021

Versión 2

ALCALDÍA MAYOR DE BOGOTÁ D.C.
INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO
BOGOTÁ

Control de Cambios		
Versión	Fecha	Descripción de la Modificación
1	28/12/2020	Versión inicial
2	12/01/2021	Se establecen definiciones y cronograma en el documento

Elaboró	Revisó	Aprobó
José Alejandro Suárez Profesional Especializado Infraestructura Oficina TICS	Paula Contreras Jefe Oficina TICS	Comité Gestión y Desempeño

CONTENIDO

1. INTRODUCCIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

DEPENDENCIA
Oficina de Tecnologías de la Información y las Comunicaciones TIC.

PROCESO
Proceso Estratégico TIC's Para la Gestión del Riesgo.

2. OBJETIVO

Elaborar el Plan de Seguridad y Privacidad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, dando cumplimiento al Decreto 612 de 2018.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información aplica a todos los procesos del Instituto Distrital De Gestión de Riesgos y Cambio Climático – IDIGER, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información - MSPI del MINTIC.

4. RESPONSABLES

Oficina de Tecnologías de la Información y las Comunicaciones

5. DEFINICIONES

Activo: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

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.

Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Privacidad de datos: La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

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 consecuencias. (ISO/IEC 27000).

Rol: Papel, función que alguien o algo desempeña.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

6. METODOLOGÍA

Para el Plan de Seguridad y Privacidad de la Información se establecen las siguientes etapas de planeación, implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI - del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER para la vigencia 2021.

a. Planeación

	Actividad	Responsable
1	Identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Oficina TIC Oficina Planeación
2	Ajustar el plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Oficina TIC
3	Elaborar procedimiento de gestión de incidentes de Seguridad de la Información	Oficina TIC
4	Establecer indicadores de Seguridad y Privacidad de la Información	Oficina TIC
5	Revisar políticas y procedimientos relacionados con el modelo de seguridad y privacidad de la información.	Oficina TIC
6	Establecer una estrategia para fomentar la cultura de la seguridad y privacidad de la información dentro de la entidad	Oficina TIC Oficina Asesora de Comunicaciones

b. Implementación

	Actividad	Responsable
1	Análisis y evaluación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Oficina TIC Oficina Planeación
2	Ejecución del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Oficina TIC
3	Publicar y socializar el procedimiento de gestión de incidentes de Seguridad de la Información	Oficina TIC

4	Reporte de indicadores de seguridad y privacidad de la información	Oficina TIC
5	Ajustar y actualizar las políticas y procedimientos relacionados con el modelo de seguridad y privacidad de la información.	Oficina TIC
6	Ejecutar la estrategia para fomentar la cultura de la seguridad y privacidad de la información dentro de la entidad	Oficina TIC Oficina Asesora de Comunicaciones

c. Seguimiento

Con el fin de realizar el manejo y seguimiento respectivo, la oficina TIC ha establecido el siguiente cronograma para verificar las actividades establecidas en el plan.

Trimestre	Fecha Programada
Primer trimestre 2021	Abril 1 a Abril 5
Segundo trimestre 2021	Julio 1 a Julio 5
Tercer trimestre 2021	Octubre 1 a Octubre 4
Cuarto trimestre 2021	Enero 6 a Enero 10 (2022)

d. Mejora Continua

Actividad	Responsable
Definir y desarrollar oportunidades de mejora	Oficina TIC
Acciones correctivas	Oficina TIC

7. RECURSOS PARA LA IMPLEMENTACIÓN DEL PLAN

Para la implementación del Plan de Seguridad y Privacidad de la Información se utilizarán los siguientes recursos

Humanos

La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua. Adicionalmente con el personal de otras subdirecciones y oficinas que se requieran para la planeación, implementación y seguimiento, debido a que es un plan transversal que involucra a toda la entidad

Técnicos

Instrumento de Evaluación de MSPI del MINTIC
Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información - MINTIC
Modelo de Seguridad y Privacidad de la Información - MINTIC

Logísticos

Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

Financieros

Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías.

8. INDICADOR DEL PLAN

(Número de actividades ejecutadas en el plan)/(Total de actividades establecidas en el plan)

9. PRESUPUESTO

La estimación y asignación del presupuesto para el Plan de Seguridad y Privacidad de la información del Instituto Distrital de Gestión del Riesgo y Cambio Climático IDIGER, corresponde al recurso humano designado para el desarrollo de las actividades planteadas.

10. NORMATIVIDAD APLICABLE

•Constitución Política de Colombia 1991 - Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

•Decreto 612 de 2018 – "Por el cual se fijan directrices para formular y adoptar el Plan de Acción por parte de las entidades del Estado"

•Decreto 1008 de 2018 – "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"

•Norma técnica Colombiana NTC/IOS 27001:2013 Sistemas de Gestión de Seguridad de la Información (SGSI)

•Modelo de Seguridad y Privacidad de la Información – MINTIC

•Resolución 149 de 2019 – "Por la cual se adopta el Marco de Referencia de Administración del Riesgo del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER"

•Resolución 214 de 2019 "Por la cual se adopta la política de seguridad y privacidad de la información"

•Manual de Políticas de Seguridad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático

11. CRONOGRAMA PRELIMINAR

ETAPA	ACTIVIDAD	FECHA (preliminar)
PLANEACIÓN	Identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Del 1 de Febrero de 2021 Hasta el 30 de Mayo de 2021
	Ajustar el plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	
	Elaborar procedimiento de gestión de incidentes de Seguridad de la Información	
	Establecer indicadores de Seguridad y Privacidad de la Información	
	Revisar políticas y procedimientos relacionados con el modelo de seguridad y privacidad de la	

	información.	
	Establecer una estrategia para fomentar la cultura de la seguridad y privacidad de la información dentro de la entidad	
IMPLEMENTACIÓN	Análisis y evaluación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Del 1 de Junio de 2021 Hasta el 30 de Septiembre de 2021
	Ejecución del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	
	Publicar y socializar el procedimiento de gestión de incidentes de Seguridad de la Información	
	Reporte de indicadores de seguridad y privacidad de la información	
	Ajustar y actualizar las políticas y procedimientos relacionados con el modelo de seguridad y privacidad de la información.	
	Ejecutar la estrategia para fomentar la cultura de la seguridad y privacidad de la información dentro de la entidad	
SEGUIMIENTO	Tercer trimestre 2021	Octubre 1 a Octubre 4
	Cuarto trimestre 2021	Enero 6 a Enero 10 (2022)
MEJORA CONTINUA	Definir y desarrollar oportunidades de mejora	Noviembre – Diciembre 2021
	Acciones correctivas	