PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TC-PL-03

Tecnologías de la Información y las Comunicaciones

31/01/2025

Versión 7

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
3	24/01/2022	Se actualiza definiciones y cronograma en el documento
4	25/01/2023	Se actualiza cronograma en el documento
5	30/01/2024	Se actualiza cronograma en el documento
6	21/03/2024	Actualización de las actividades incluidas en el Plan de acuerdo con el Diagnóstico realizado.
7	31/01/2025	Actualización de las actividades incluidas en el Plan de acuerdo con el Diagnóstico realizado

Elaboró	Revisó	Aprobó
Carmenza González Vargas Profesional Universitario Claudia Marcela Ladino Jefe Oficina Tecnologías de la Información y las Comunicaciones	Claudia Marcela Ladino Jefe Oficina Tecnologías de la Información y las Comunicaciones Nelson Jairo Rincón Martínez Jefe Oficina Asesora de Planeación	Comité Institucional de Gestión y Desempeño

Tabla de contenido

1. Introducción

El IDIGER, se encuentra en el proceso de dar continuidad y alcanzar un nivel de madurez óptimo del Sistema de Gestión de Seguridad de la Información- SGSI, el cual le permite preservar la confidencialidad, integridad, y disponibilidad de la información, dando cumplimiento normativo a la legislación, políticas y lineamientos relacionados con la administración y protección de información, las cuales aplican a las entidades estatales. En cumplimiento de la Política de Gobierno Digital y la Política de Seguridad y Privacidad de la Información y del Modelo de Seguridad y Privacidad de la Información – MSPI elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, acoge los lineamientos para la implementación de la estrategia de seguridad digital en las entidades públicas, mediante la implementación del Sistema de Gestión de Seguridad de la Información.

2. Normograma

- ✓ Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- ✓ Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes.
- ✓ Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- ✓ Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- ✓ Ley 1712 de 2014. 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.
- ✓ Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital.
- ✓ Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- ✓ CONPES 3995 de 2020. Confianza y Seguridad Digital
- ✓ CONPES 3854 de 2017. Política Nacional de Seguridad digital.

- ✓ CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- ✓ Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

- ✓ Resolución 419 12 de octubre de 2023 "Por la cual se actualiza la Política General de Seguridad de la Información y Seguridad Digital, y se definen lineamientos frente al uso y manejo de la información del Instituto Distrital de Gestión de Riesgos y Cambio Climático - IDIGER."

- ✓ Acuerdo N0 002 de 22 de diciembre de 2023 "Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad".

3. Definiciones

ISO: Sigla de International Standard Organization.

MINTIC: Ministerio de Tecnología de la Información y las Comunicaciones.

MSPI: Modelo de Seguridad y Privacidad de la Información.

SGSI: Sistema de Gestión de Seguridad de la Información, el cual pertenece al conjunto de normas ISO.

TIC: Tecnologías de la información y la comunicación.

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. (ISO/IEC 27000).

ACTIVO DE INFORMACIÓN: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. (CONPES 3854 de 20116).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (GTC-ISO/IEC27035, 2012).

PARTES INTERESADAS: 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 ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.

RIESGO POSITIVO: Posibilidad de ocurrencia de un evento o situación que permita optimizarlos procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

SEGURIDAD DE LA INFORMACIÓN: Este principio 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.

4. Políticas de MIPG

MIPG es el marco de referencia que tienen las entidades públicas para llevar a cabo sus procesos de gestión institucional, cuyos lineamientos se han emitido a través de las políticas de gestión y desempeño previstas en el Decreto 1083 de 2015 y sus respectivas modificaciones al respecto.

Las políticas POL 07 y 08: Gobierno Digital y Seguridad Digital, nos brindan los lineamientos para implementar dichas políticas. Gobierno Digital: Seguridad y Privacidad de la información y Seguridad Digital: Asignación de Recursos, Despliegue de controles, Implementación Lineamientos de la Política.

5. Objetivo General

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información –MSPI de la política de Gobierno Digital del MinTIC, alineadas con la NTC/IEC ISO 27001, la Política pública de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información de los procesos del IDIGER.

6. Objetivos Específicos

6.1. Definir y aplicar los lineamientos para tratar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) para alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

6.2. Establecer el conjunto de actividades necesarias para el tratamiento de riesgos del modelo de seguridad y privacidad de la información - MSPI, sobre los activos de tecnologías de información que soportan la prestación de servicios digitales de la Entidad, frente a Ciber amenazas y otros tipos de eventos de seguridad de la información, fortaleciendo la confianza de los ciudadanos, usuarios y demás partes interesadas.

7. Planificación de la ejecución del Plan

La Oficina de Tecnologías de la Información y las Comunicaciones, como primera línea de defensa, será responsable de la planificación del presente plan. Para ello, elaborará los autodiagnósticos necesarios para identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. En la elaboración de los autodiagnósticos, se tendrá en cuenta la auditoria, diagnósticos de FURAG.

8. Implementación del Plan

El Plan de Seguridad y Privacidad de la Información (PSPI) es un documento que establece las acciones necesarias para proteger la información de la organización. La ejecución de estas acciones se desarrollará de acuerdo con el cronograma de la Tabla 1, que se elaboró como resultado de las revisiones de las auditorías internas y los diagnósticos realizados por el área de TIC. El propósito de la ejecución de estas actividades es garantizar la seguridad y privacidad de la información.

9. Responsable del seguimiento del Plan

Monitoreo: La Oficina Asesora de Planeación, como la segunda línea de defensa, será responsable de monitorear el PSPI.

Seguimiento: La Oficina de Control Interno, como la tercera línea de defensa, será responsable de seguir el PSPI y reportar su seguimiento a la Oficina Asesora de Planeación.

10. Mejoramiento continuo

Mantener la seguridad de la información requiere no solo de la implantación de un Sistema de Gestión de Seguridad de la Información, sino que se deberá realizar un mantenimiento y mejora de las medidas de seguridad.

La norma ISO 27001 constituye una solución de mejora continua muy apropiada para evaluar los distintos riesgos y establecer las estrategias y controles oportunos que permitan asegurar la protección y defender la información. Cuando se ha realizado la evaluación de los riesgos y son aplicados a los controles, siempre queda lo que se

conoce como riesgo residual que tendrá que ser revisado por lo menos una vez al año para tomar las medidas preventivas oportunas.

11. Detalle del Plan

El detalle del Plan contiene: Actividades a ejecutar, responsable principal de la ejecución del plan, dependencia(s) responsable(s) de ejecutar la actividad, mes o meses de ejecución. Mediante el plan se realizará la ejecución mensual de la primera línea de defensa, el monitoreo trimestral de la segunda línea de defensa y el seguimiento trimestral de la tercera línea de defensa.

Tabla 1 Detalle del Plan de Seguridad y Privacidad de la Información

N°	ACTIVIDAD	FASE	RESPONSABLE	T1	T2	T3	T4
1	Diligenciar autodiagnóstico de Gobierno Digital 2024 y presentar sus resultados ante el Comité Institucional de Gestión y Desempeño (CIGD).	Diagnóstico	Oficina de Tecnología de la Información y Las comunicaciones.				
2	Revisar e identificar la documentación necesaria para dar cumplimiento a la Política de seguridad y privacidad de la información.	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				
3	Realizar el reporte y seguimiento a los riesgos de seguridad de la información.	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				
4	Realizar el análisis de vulnerabilidades.	Mejoramiento continuo	Oficina de Tecnología de la Información y Las comunicaciones.				
5	Plan de Continuidad de Negocio de TI: ejecutar las actividades planteadas para el 2025.	Mejoramiento continuo	Oficina de Tecnología de la Información y Las comunicaciones.				
6	Implementar alguna actividad resultado del Diagnóstico de Datos Personales	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				
7	Implementar alguna actividad resultado del Autodiagnóstico de FURAG y MSPI	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				
8	Actualizar y reformular el plan de seguridad de la información para la vigencia 2026 basado en los resultados de los autodiagnósticos.	diagnóstico	Oficina de Tecnología de la Información y Las comunicaciones.				

9	Crear la matriz de partes interesadas que atiendan las necesidades y expectativas en seguridad de la información.	Planificación	Oficina de Tecnología de la Información y Las comunicaciones.				
10	Validar con la Subdirección Corporativa - Talento Humano y la Oficina Juridica la viabilidad de la implementación de cláusulas de seguridad y privacidad de la información en los contratos en el momento de la vinculación y terminación de los colaboradores de la entidad.	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				
11	Elaborar el documento para el etiquetado de documentos, de la clasificación en términos de confidencialidad para implementar el lineamiento de la Política de Seguridad de la Información asociada.	Operación	Oficina de Tecnología de la Información y Las comunicaciones.				

Fuente: Elaboración propia

12. Presupuesto

Los recursos disponibles corresponden a $ 500.000.000, para el desarrollo de este plan, definidos en el proyecto de inversión "*Renovación Tecnológica de la Infraestructura que Apoya el Seguimiento de los Riesgos de Desastres y del Cambio Climático y sus Efectos*".

13. Cronograma

Anexo Cronograma Plan de Seguridad y Privacidad de la Información (Formato DE-FT-63)